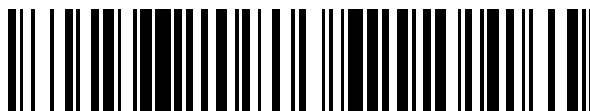


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 538 786**

51 Int. Cl.:

H04W 8/26 (2009.01)

H04W 12/04 (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **17.04.2009** **E 09749525 (3)**

97 Fecha y número de publicación de la concesión europea: **11.03.2015** **EP 2283666**

54 Título: **Procedimiento para personalización por aire de tarjetas de chip en telecomunicaciones**

30 Prioridad:

23.05.2008 DE 102008024798

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

24.06.2015

73 Titular/es:

**DEUTSCHE TELEKOM AG (100.0%)
Friedrich-Ebert-Allee 140
53113 Bonn, DE**

72 Inventor/es:

KALINER, STEFAN

74 Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

ES 2 538 786 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

Procedimiento para personalización por aire de tarjetas de chip en telecomunicaciones

5 La invención se refiere a un procedimiento para la puesta en marcha y personalización de un módulo de identificación de abonado SIM.

10 Las tarjetas de chip se usan en telecomunicaciones, en particular, por ejemplo, en los sistemas móviles GSM o UMTS para la identificación inequívoca y segura de los abonados y también para poner a disposición numerosas funciones especiales y servicios de valor agregado. Las tarjetas chip o las aplicaciones de tarjetas chip (denominadas en conjunto como "SIM" o con el mismo significado como módulo de identificación de abonado) se denominan, por ejemplo, UICC, SIM, USIM, R-UIM o también como ISIM dependiendo de la generación de tipo del estándar del sistema de base que incluye un sinnúmero de parámetros especiales, claves secretas y otros elementos del tipo más variado, por ejemplo con referencia al operador de red, proveedor, producto o abonado.

15 Para la puesta en servicio de un equipo terminal móvil y abonarlo a un servicio de radiotelefonía móvil, un SIM con datos individuales determinados - al menos identidad del abonado IMSI, clave secreta K y parámetros individuales para el algoritmo de autenticación - son necesarios forzosamente. Los elementos coincidentes deben estar presentes en las bases de datos de los abonados (por ejemplo HLR/AC o HSS) de la red local, de otra manera no es posible establecer una conexión, ni desde el abonado ni desde la red.

20 La carga de las SIM y el estampado de los datos individuales se producen en el margen de la fabricación de tarjeta en la denominada personalización, en cualquier caso mucho antes de que se utilice el módulo de identificación de abonado SIM. La cadena de valor de la disponibilidad de tarjeta se representa generalmente como sigue:

- 25
- Fabricante del chip: Fábrica el chip con (partes del) programa operativo.
 - Fabricante de tarjeta: Fabrica el cuerpo de tarjeta, implanta el chip, carga, dado el caso, otras partes no individuales del programa de operación y datos correspondientes.
 - 30 • Personalizador: Carga datos más individualizados, indicativos individuales de abonado, claves secretas y, dado el caso, partes individuales del programa (aplicaciones) adicionales. Intercambia datos individuales con el operador de red. Por regla general es idéntico con el fabricante de tarjetas.
 - 35 • Empacador/ distribuidor: Empaca y envía las tarjetas chip personalizadas al operador de red u otros destinos. Puede ser idéntico con el fabricante de tarjetas y/o el personalizador.
 - Operador de red: Opera la red de comunicaciones. Define la personalización de sus productos, suministra todas las especificaciones al personalizador, recibe datos individuales (al menos IMSI, K y parámetros individuales del algoritmo de autenticación) del personalizador para establecer en sus bases de datos las condiciones del abonado.
- 40

45 Al final del proceso de suministro, los SIM se encuentran en los puntos de venta del operador de red. Sólo al finalizar un contrato de radiotelefonía móvil se produce en el margen de la denominada activación la asignación al cliente concreto y la adjudicación de un número telefónico. La activación requiere la existencia de la condición del abonado en las bases de datos del operador de red.

Como desventaja de esta cadena de proceso, en particular la personalización centralizada, se debe indicar:

- 50
- Especialización e individualización del producto de manera temprana en la cadena de disponibilidad; en este momento sólo es posible estimar la necesidad real.
 - Absorción de recursos (capacidad de base de datos y números) del operador de red se produce, en parte, mucho antes de la necesidad real.
 - Una prestación del servicio muy especial con soluciones técnicamente complejas y una flexibilidad limitada.
 - 55 Un gasto elevado para la asistencia del personalizador externo. Por regla general, las modificaciones se ordenan después del ofrecimiento, después son desarrollados, probados y aceptados, todo con el tiempo necesario. La flexibilidad necesaria requiere interfaces complejas.
 - Grandes dificultades en el manejo de desarrollos nuevos de SIM, por ejemplo variantes no extraíbles o "máquina a máquina" (M2M). Genera una especialización desfavorable ya en los productos preliminares.
 - 60 Freno a la innovación.
 - Con la personalización convencional los conceptos "soft" alternativos para los SIM son completamente imposibles.

Por la patente estadounidense 7.266.371 B1 se conoce un procedimiento para la activación de una terminal de radiotelefonía móvil en el cual una tarjeta SIM es equipada de parámetros operativos temporarios, en particular un número temporario de identificación de abonado (IMSI) que se usan para un primer acceso a la red de radiotelefonía móvil. Después de haber establecido una comunicación con la red de radiotelefonía móvil mediante dichos parámetros, el usuario se puede suscribir a través del terminal de radiotelefonía móvil a una serie de servicios y realizar un procedimiento de activación en el cual se almacenan parámetros operativos permanentes sobre la tarjeta SIM, en particular un número permanente de identificación de abonado (IMSI)

Un procedimiento similar se describe en la solicitud internacional de patente WO 03/077585 A1 y de la solicitud de patente europea EP 1 895 791 A1, en el cual, en este caso, antes de la puesta en funcionamiento se transmite un código de abonado (IMSI) a un sistema de gestión de red y un distribuidor de tarjetas SIM le adjudica una dirección de comunicación (MSISDN) y la transmite también junto con el código de abonado (IMSI) al sistema de gestión de red. Entonces, la tarjeta SIM, por medio de un equipo terminal, hace contacto con el sistema de gestión de red, por lo cual el mismo recibe nuevamente la dirección de comunicación (MSISDN) y el código de abonado (IMSI). A continuación, el mismo asigna a la tarjeta SIM un código definitivo de abonado que le es enviada al equipo terminal mediante una información, en particular un SMS. El equipo terminal extrae entonces el código definitivo de abonado y lo almacena en la tarjeta SIM.

Además, la solicitud internacional de patente WO 02/058361 A1 describe un procedimiento para la activación de un equipo terminal móvil. En este procedimiento, adicionalmente al indicativo o indicativos temporarios/s de la tarjeta SIM o almacenado/s en la misma se usa un número electrónico de serie temporario para identificar el equipo terminal durante el proceso de activación. La red reconoce que es un número electrónico de serie temporario e inicia un proceso de activación. A{ continuación, el indicativo temporario o los indicativos temporarios es/son sobrescrito/s.

En el procedimiento mencionado es desventajoso que, además de los códigos definitivos de abonado también sea unívoco el código provisorio de abonado y el número electrónico de serie y con ello se produce tempranamente una absorción de recursos. Además es necesaria una administración de los indicativos temporarios informando, antes de la emisión de tarjetas SIM, a los abonados de una determinada instancia en la red.

Por lo tanto, el objetivo de la invención es perfeccionar un procedimiento para la puesta en servicio y personalización de un módulo de identificación de abonado (SIM) de tal manera que supere las desventajas del procedimiento según el estado actual de la técnica, y, en particular, permita que sin una tipificación temprana de recursos, tal como una capacidad de base de datos y números sea posible, en cualquier momento, una disponibilidad personalizada y módulos de identificación de abonado (SIM) liberados para el funcionamiento en una red de radiotelefonía móvil de abonados (SIM) correspondiente a la demanda actual.

Este objetivo se consigue según la invención mediante un procedimiento de acuerdo con la reivindicación 1. Otras configuraciones ventajosas del procedimiento según la invención se indican en las reivindicaciones secundarias.

Es particularmente ventajoso que el procedimiento según la invención para la puesta en servicio y personalización de un módulo de identificación de abonado, en adelante SIM, el SIM sea equipado antes de la primera puesta en servicio de un registro (S*) no individual y provisorio de parámetros iniciales de identificación y autenticación que contienen al menos una identificación de abonado (IMSI*) no individual y provisorio y una clave secreta (K*) no individual y provisorio, permitiendo el registro paramétrico (S*) una primera puesta en servicio del SIM en una red de radiotelefonía móvil mediante una terminal de radiotelefonía móvil, siendo realizada una personalización después de la primera puesta en servicio del SIM mediante la transmisión de un registro de datos de abonado (S) individual y definitivo y su almacenamiento en el SIM, incluyendo una identificación de abonado (IMSI) inequívoca definitiva y una clave secreta (K), y con lo cual el registro de datos de abonado(S), en particular el definitivo sea transmitido por medio de un enlace regular del sistema de radiotelefonía móvil usando el (S*).

El registro provisional (S*) de parámetros iniciales de identificación y autenticación incluye, por lo tanto, al menos una identificación de abonado (IMSI*) no individual y provisorio y una clave secreta (K*) no individual y provisorio, permitiendo el registro paramétrico (S*) una primera puesta en funcionamiento del SIM en una red de radiotelefonía móvil mediante una terminal de radiotelefonía móvil, es decir que tanto la identificación de abonado como la clave secreta en su carácter de componentes del registro provisorio (S*) de parámetros iniciales de identificación y autenticación no son individuales y solamente provisorios.

De esta manera es, primeramente, posible equipar un sinnúmero de módulos de identificación de abonados SIM (Subscriber Identity Module), que permitan un uso de los servicios de una red de radiotelefonía móvil, de registros paramétricos no individuales y provisionales, sin que ya deban ser asignados un número correspondiente de recursos, por ejemplo identidades de abonados IMSI y números de radiotelefonía móvil MSISDN asignados inequívocamente, puesto que el conjunto provisional de datos paramétricos permite una primera puesta en servicio, es decir abonarse a una red de radiotelefonía móvil y, a continuación, se realice por el lado de la red la personalización del SIM generando un registro definitivo de datos de abonado, sea transmitido por medio de la conexión radiotelefónica existente y almacenado en el SIM. De esta manera, los datos de abonado finales que se

almacenan en el SIM y se utilizan en la identificación de abonado en el uso de los servicios de la red de radiotelefonía móvil se transmiten al SIM en el margen de un proceso estándar (por aire – OTA). De esta manera, los recursos existentes y las capacidades de red también se aprovechan ventajosamente.

- 5 La presente invención posibilita desplazar la personalización, en términos de espacio, del personalizador externo al dominio del operador de red y, en términos de tiempo, al final de la cadena de la puesta a disposición en el momento ideal de la primera puesta en servicio del equipo terminal móvil.

10 Mediante el procedimiento sugerido se consigue generar para un sistema de comunicaciones módulos de identificación de abonados (SIM) completamente sin datos individuales (abstracción hecha de, por ejemplo, un número de serie consecutivo) y suministrarlos. En este momento, mantienen en vez de esto datos de identificación especiales no individuales y temporarios, los cuales, sin embargo incluso así, vuelven posible una conexión a la red del operador, en línea con los estándares. Mediante los mecanismos por aire se produce entonces la personalización individual de los parámetros definitivos de la condición del abonado y demás configuración dedicada del SIM con datos y aplicaciones. El diseño tecnológico de la tarjeta permite, además, la repetición ilimitada del proceso (repersonalización, incluso en el margen de un cambio de operador de red) y siempre la posibilidad de cambiar todos los datos relevantes en cualquier momento y de la misma manera. En detalle, las ventajas son las siguientes:

- 20 • La configuración individual del SIM se produce en el momento lo más tarde posible, hasta entonces la gran flexibilidad respecto de la utilización del SIM se mantiene.
- Puesto que no se lleva a cabo personalización individual dentro del margen de la producción de tarjeta, este paso del proceso puede ser omitido, sin sustitución. Se evitan las desventajas mencionadas del estado actual de la técnica.
- 25 • La interfaz con el fabricante de tarjetas se simplifica considerablemente, gracias a que ahora ya no es necesario transmitir parámetros de personalización y ya no son retornados datos individuales críticos para la seguridad.
- En el margen de la fabricación de tarjetas no existe ninguna creación de fichero en las bases de datos del operador de red y, con ello, tampoco ninguna absorción de recursos mucho antes de la necesidad real.
- 30 • Fundamentalmente, no es necesario el almacenamiento de datos individuales, ni en el fabricante de tarjetas ni en el operador de red o un tercero.
- Las alternativas modernas respecto del SIM convencional se tornan posibles y obtienen un atractivo adicional: En el uso de módulos no extraíbles o módulos "M2M", es posible prescindir, adicionalmente, del fabricante de tarjetas, puesto que el fabricante del chip puede suministrar directamente. En el caso de conceptos Soft, en la cadena de suministros incluso se prescindiría del fabricante de chips.
- 35 • La infraestructura de la que de todos modos debe disponer el operador de red para una comercialización por aire selectiva del SIM (cuando, por ejemplo, el equipo terminal y la tarifa del cliente están establecidos) se hace cargo de la tarea de personalización y es aprovechado de manera más efectiva. De esta manera se producen efectos sinérgicos.

40 Los diseños novedosos del SIM que, de todos modos presuponen o causan implícitamente modificaciones en el modelo de transferencias de transmisión (por ejemplo, variantes mecánicas incorporadas, soldadas o realizadas dentro de software) pueden poner en juego sus ventajas tanto mejor cuanto más tarde sean individualizados y especializados. Estas variantes ya no llegan, por regla general, a las manos del usuario y se convierten en
45 componente permanente de un equipo terminal mucho antes de conocerse el operador de red. Además, el mismo puede cambiar durante el ciclo de vida del equipo terminal. Es así que en la discusión respecto de las formas futuras del SIM surge regularmente la cuestión de la repersonificación. Además, sería ideal hasta el momento de la puesta en servicio una independencia amplia de un operador de red para, a ser posible, permitir una producción sencilla, sin interfaces complicadas, la administración de áreas numéricas específicas del operador, algoritmos de autenticación propietarios, etc. La presente invención posibilita, precisamente, dichas características importantes, estando en cada momento determinado el operador local inicial (o un grupo de operadores), pero ya no requiere una coordinación de datos individuales. No obstante, el operador de red continúa teniendo por medio de la personalización selectiva todas las posibilidades de influencia y diseño que nadie, excepto él mismo, puede realizar.

55 Las tarjetas chip según la invención están equipadas, preferentemente, de un registro no individual de parámetros iniciales de identificación y autenticación

$$S^*_i = \{IMS^*_i, K^*_i, Qc^*_i, OK^*_i \text{ con } i = 0, 1, \dots, N-1 \text{ y } N \ll M$$

60 con lo cual IMS^*_i puede contener el indicativo de red MCC y MNC del operador. N es la cantidad total de S^*_i y M la cantidad de los SIM producidos en total de esta manera para un operador de red. Dentro de M se repiten los S^*_i o sea M/N veces y, de esta manera, son no unívocos y no individuales.

Como única característica individual es posible, por ejemplo, agregar el número de serie (ICCID) habitual, asignado por el fabricante de manera consecutiva durante la producción. Lo importante es que todos los datos a asignar durante el proceso de producción en marcha sean otorgados de manera completamente automática y sin especificaciones especiales (individuales) del operador de red.

En particular, además, no se produce ningún almacenamiento o transferencia de datos individuales por parte del fabricante del SIM, operador de red o un tercero.

En la red de radiotelefonía móvil del operador existe una base de datos especial (THLR) del tamaño fijo N con los S^*_i y, en cada caso, un número telefónico MSISDN $_i$ asignado definitivamente. Las condiciones de abonados en esta base de datos son invariables, en particular no existe ninguna conexión con el fabricante de las tarjetas chip.

Un SIM asociado es ahora puesto en servicio por primera vez en un equipo terminal móvil completamente estándar (es decir, equipado sin precauciones especiales respecto del procedimiento aquí descrito). Después de la primera puesta en servicio con S^*_i se produce la transmisión de los datos definitivos de abonado (S) que están almacenados en el módulo de identificación de abonado SIM. Al mismo tiempo, estos datos definitivos de abonado son guardados también en el registro de localización geográfica de abonados HLR. El módulo de identificación de abonado SIM está entonces en condiciones operativas con los datos definitivos.

Preferentemente, con la primera puesta en servicio, el establecimiento de una comunicación con un servidor de personalización (PS) se produce dentro de la red de radiotelefonía móvil, siendo por parte del servidor de personalización (PS) generado el registro de datos de abonado (S) individual y definitivo para la personalización y transmitido al SIM, en particular usando los datos de abonado (S^*_i) no individuales y provisionales.

Según la invención, la identificación de abonado provisional (IMSI $_i$) no es inequívoca y adjudicada provisionalmente a varios módulos de identificación de abonados (SIM). DE esta manera es posible de cuidar los recursos existentes, por ejemplo, reusando cíclicamente los registros paramétricos, pudiendo, sin embargo, los SIM permanecer identificables y diferenciables mediante una identificación inequívoca, por ejemplo el número de serie.

En una forma de realización preferente, antes de la realización de la personalización se procede a una comprobación de los números de serie del SIM (ICCID) y/o del terminal de radiotelefonía móvil mediante el número de identidad del equipo (IMEI) mediante el cual el terminal de radiotelefonía es identificable inequívocamente, y/o una comprobación de otros parámetros de seguridad del SIM. De esta manera, es posible aumentar la seguridad del procedimiento.

Según la invención, el número de registros de datos de abonado (S^*) posibles que contienen al menos una identificación de abonado (IMSI *) no individual y provisional y una clave secreta (K^*) no individual y provisional es establecido y menor, en particular muy menor que el número de la totalidad de los módulos de identificación de abonados (SIM) equipados con dichos registros de datos (S^+), existiendo en todo momento muchos módulos de identificación de abonados (SIM) con datos provisionales (S^*) idénticos.

De manera particularmente preferente, los registros de datos de abonado (S^*) no individuales y provisionales, conteniendo al menos una identificación de abonado (IMSI *) no individual y provisional y una clave secreta (K^*) no individual y provisional son reusados cíclicamente en la configuración inicial de los módulos de identificación de abonados (SIM), en particular independientemente de si o cuantos de los SIM ya han sido personalizados con datos de abonado (S) personalizados y definitivos.

Así, es posible garantizar una distribución uniforme de los registros de datos de abonado (S^*) provisionales y no definitivos, de manera que no se llega a producir a una acumulación accidental de uno o más registros de estos registros de abonados (S^*) no individuales. De esta manera se puede reducir el riesgo de una colisión debida al uso simultáneo casual del mismo registro de datos de abonado provisional en dos diferentes tarjetas SIM, es decir módulos de identificación de abonados.

Preferentemente, después de la recepción y el definitivo almacenamiento del registro de abonados (S) sobre el (SIM) (recepción del registro de datos de abonado) se transmite una confirmación desde el terminal de radiotelefonía móvil a la red de radiotelefonía móvil. Preferentemente, se ejecuta un reinicio en caliente de la terminal de radiotelefonía usando el nuevo registro de datos de abonado (S). Mediante la confirmación de la correcta recepción de datos, la red de radiotelefonía móvil recibe del SIM un acuse de recibo de la personalización, de manera que el proceso puede ser concluido.

Preferentemente, el registro de datos de abonado (S) generado en la personalización es almacenado en el registro de localización geográfica de abonados (HLR) El almacenamiento del registro de datos de abonado (S) y de los datos de abonado correspondientes en el registro de localización geográfica de abonados (HLR) permite el uso de los servicios de la red de radiotelefonía móvil.

En este caso, la condición de abonado puede estar provista, primeramente, de restricciones de servicios específicos, que son levantadas sólo más tarde, después de determinar los datos del cliente, servicios requeridos, etc.

Preferentemente, durante la primera puesta en servicio con el registro de parámetros (S*) la condición de abonado proporcionada por el (IMSI*) por el lado de la red es puesta en un estado "en uso", mientras tanto está liberado solamente un uso restringido, en particular la realización de la personalización, con lo cual después de la personalización del SIM realizada mediante el registro de datos de abonado (S) individual y definitivo la condición de abonado proporcionada por el (IMSI*) es colocada en un estado "liberado" que permite el uso renovado de la condición de abonado proporcionada por el (IMSI*) mediante otro módulo de identificación de abonado SIM.

De manera particularmente preferente, en un intento de puesta en servicio de uno o más SIM adicionales con un registro paramétrico (S*) provisional idéntico con un primer SIM ya registrado en la red de radiotelefonía móvil se produce una primera incorporación a una cola de espera y un procesamiento según el orden cronológico de los intentos de puesta en servicio. Preferentemente, en un intento de puesta en servicio de uno o más módulos de identificación de abonados (SIM) adicionales mediante una identificación de abonado (IMSI*) provisional idéntica a un primer módulo de identificación de abonados (SIM) ya registrado para la personalización en la red de radiotelefonía móvil, el módulo de identificación de abonado (SIM) detecta un bloqueo eventual del proceso de personalización (falta de datos de personalización) y produce la repetición automática del requerimiento de personalización.

Preferentemente, en un intento de puesta en servicio de uno o más módulos de identificación de abonados (SIM) adicionales mediante una identificación de abonado (IMSI*) provisional idéntica a un primer módulo de identificación de abonados (SIM) ya registrado para la personalización en la red de radiotelefonía móvil, el módulo de identificación de abonado (SIM) detecta un error de direccionamiento eventual de los datos de personalización, los datos son desechados y se produce la repetición automática del requerimiento de personalización.

De manera particularmente preferente, ante la falta la confirmación del terminal de radiotelefonía móvil a la red de radiotelefonía móvil se produce automáticamente un nuevo envío de los datos de personalización. Preferentemente, sólo después de la confirmación del terminal de radiotelefonía móvil a la red de radiotelefonía móvil se produce el almacenamiento del registro de datos de abonado (S) definitivo en el registro de localización geográfica de abonados (HLR).

Preferentemente, sólo después de la confirmación del terminal de radiotelefonía móvil a la red de radiotelefonía móvil se produce la activación y/o liberación de la condición de abonado (suscripción) caracterizado por el registro de datos de abonado (S) definitivo en el registro de localización geográfica de abonados (HLR).

De manera particularmente preferente, los registros de datos de abonado (S) ya han sido creados a corto plazo provisionalmente en el registro de localización geográfica de abonados (HLR). De esta manera se garantiza que una personalización de módulos e identificación de abonados (tarjetas SIM) puede ser realizada a corto plazo en cualquier momento.

De manera preferente, las condiciones de abonado (suscripciones) definitivas caracterizadas mediante los registros de datos de abonado (S) definitivos ya han sido creados a corto plazo provisionalmente en el registro de localización geográfica de abonados (HLR).

De manera particularmente preferente, mediante los registros de datos de abonado (S) definitivos en el registro de localización geográfica de abonados (HLR), las condiciones de abonados (suscripciones) ya han sido provistas de restricciones de servicio específicas.

Preferentemente, los procesos de carga adicionales para la configuración de la tarjeta SIM con propiedades y/o servicios particulares se producen automáticamente a continuación de la personalización realizada.

Preferentemente, a continuación de la personalización realizada se inicia automáticamente un diálogo mecánico o personal con el cliente, preferentemente a través de la terminal de radiotelefonía móvil, para el chequeo de datos del cliente, requerimientos de servicios, etc. y, particularmente, sólo después se eliminan las eventuales restricciones de servicio específicos.

Se muestra en las figuras y explica a continuación un ejemplo de realización del procedimiento según la invención. Muestran:

La figura 1, un ejemplo de realización del procedimiento según la invención de la personalización por aire de un módulo de identificación de abonado SIM;

la figura 2, el esquema de la puesta en servicio simultánea de múltiples SIM, en particular con registro paramétrico provisional idéntico.

Las tarjetas chip (SIM) están provistas de un conjunto no individual de parámetros de identificación y autenticación iniciales

$S_i^* = \{IMS_i^*, K_i^*, OPC_i^*, QC_i^*, OK_i^*\}$ con $i = 0, 1, \dots, N-1$ y $N \ll M$; donde IMS_i^* contiene el indicativo válido MCC y MNC del operador. N es la cantidad total de S_i^* y M la cantidad de los SIM producidos de esta manera en total para un operador de red. Dentro de M se repiten los S_i^* o sea M/N veces y, de esta manera, son no inequívocos y no individuales.

Como única característica individual se agrega el número de serie (ICCID) habitual, asignado de manera consecutiva por el fabricante durante la producción. Lo importante es que todos los datos a asignar durante el proceso de producción en marcha sean otorgados de manera completamente automática y sin especificaciones especiales (individuales) del operador de red.

En la red de radiotelefonía móvil del operador existe una base de datos especial (THLR) del tamaño fijo N con los S_i^* y, en cada caso, un número telefónico $MSISDN_i^*$ fijo asignado. Las condiciones de abonados en la base de datos son invariables, en particular no existe ninguna conexión con el fabricante de las tarjetas de chip.

Un SIM asociado es ahora puesto en servicio por primera vez en un equipo terminal móvil completamente estándar (es decir, equipado sin precauciones especiales respecto de la presente propuesta). Simplificando las demás transacciones de sistema en la suscripción a una red de radiotelefonía móvil se produce la personalización según la representación de la figura 1:

(1) La IMS_i^* es leída por el terminal móvil y de manera estándar transmitida a la red de radiotelefonía móvil receptora, de ésta, dado el caso, a la red local y dentro de la misma al THLR. La información de routing necesaria para ello es tomado de IMS_i^* . La IMS_i^* es conocida por el THLR y, de acuerdo con el protocolo normal de autenticación, está dispuesto entre la tarjeta y el THLR con los datos S_i^* . El resultado es positivo y la relación de abonado pasa de manera estándar al estado en el cual es posible el establecimiento bilateral de una comunicación. Como función especial, el THLR proporciona al IMS_i^* el estado de "en uso" en el plazo más breve posible. Dicho estado permanece vigente hasta la liberación de la IMS_i^* , mediante la conclusión correcta de la personalización subsiguiente o bien la aparición de un caso especial (véase más adelante).

(2) En el lado de red se procede ahora a iniciar la personalización por aire, es decir la transferencia de los datos personalizados de abonado a través de una comunicación radiotelefónica, suministrando el subíndice i al servidor de personalización PS. El PS conoce para el subíndice i la $MSISDN_i^*$ apropiada y la clave por aire OK_i^* . Ahora establece, de acuerdo con el estado actual de la técnica, una sesión por aire segura con el SIM respectivo. Ahora, en primer lugar, es posible, por ejemplo, consultar el ICCID de la tarjeta o IMEI del equipo (por ejemplo mediante una lista blanca o negra) y/u otros parámetros de seguridad de la tarjeta (por ejemplo, un certificado) antes de iniciar la personalización real. Con este propósito se genera en el PS los datos definitivos de abonado

$S = \{IMS_i, K, OPC, QC, OK\}$

enviados a través del canal por aire existente al SIM y almacenados allí – de esta manera, la tarjeta es personalizada individualmente.

(3) El proceso es soportado apropiadamente en el lado de la tarjeta y asegurado de tal manera que los errores de conexión o una recepción sólo parcial no puedan conducir a una personalización incompleta (y, por lo tanto, inválida). Sólo después de una recepción completa y correcta y el almacenamiento de todos los datos necesarios, el SIM acusa recibo al PS y dispone, finalmente, un reinicio en caliente (full refresh) del equipo terminal, ahora con los datos definitivos de abonado S .

(4) En paralelo con la personalización del SIM, el PS dispone la creación de la relación de abonado S en el HLR definitivo. Con ello se ha conseguido en ambos lados un estado como después de una personalización y configuración convencionales. El SIM puede ser usado ahora para la operación estándar.

Preferentemente, el almacenamiento y la activación de las condiciones definitivas de abonado S en el registro de localización geográfica de abonados HLR pueden llevarse a cabo solamente después de haberse obtenido el acuse de recibo del SIM a la red de radiotelefonía móvil y ser provisto transitoriamente de restricciones de servicios específicas.

Para la aceleración del proceso, las condiciones definitivas de abonado S en el HLR ya pueden ser creados provisionalmente a corto plazo, por ejemplo que el PS previsoriamente almacene o active regularmente en el HLR un número de condiciones de abonados S para las necesidades urgentes (por ejemplo, para la hora siguiente o el día siguiente).

(5) El acuse de recibo del SIM obtenido en (3) lleva en el PS y la THLR a la liberación inmediata de la condición de

abonado S_i^* , en particular IMS_i^* . Cambia del estado "en uso" al estado "libre" y está así disponible para el uso siguiente.

De hecho, debido a la naturaleza no inequívoca de los registros paramétricos S_i^* y el carácter fortuito de las puestas en servicio, incluso con distribución uniforme de los S_i en la cantidad total producida (que es conseguida mediante el sencillo incremento de i durante la producción), debe contarse con colisiones durante la personalización por aire. Esto es el caso cuando durante el procesamiento de la condición de abonado S_i^* , es decir cuando el IMS_i^* está caracterizado como "en uso", se produce un segundo o incluso más intentos de suscripción de otros SIM con idéntico registro de datos paramétricos S_i^* . Este caso se muestra en la figura 2.

Sin embargo, tales colisiones presuponen un caso operativo regular que es tenido en cuenta como sigue:

- Los intentos de abono no procesados inmediatamente con IMS_i^* son incorporados en la cola de espera y procesados en la secuencia de la incorporación.
- El número N de los registros paramétricos S_i^* deben ser escogidos de tal manera que la probabilidad de una colisión (y sobre todo una colisión múltiple) sea suficientemente pequeña. Debido a que $N \ll M$ continúa siendo válida, las ventajas de la presente propuesta se mantienen completamente, incluso con $N = 1.000$ o $N = 10.000$.
- La velocidad de la personalización por aire debe ser configurada mediante sistemas optimizados, de tal manera que el intervalo de tiempo en uso de un IMS_i^* sea, a ser posible, reducido.
- Los casos de error durante el ciclo de personalización, por ejemplo al faltar el acuse de recibo del SIM, deben ser limitados mediante el time-out, de manera que el IMS_i^* sea, de ser posible, liberado nuevamente.
- Un bloqueo eventual del proceso de personalización (falta de los datos de personalización) es detectado por el SIM y conduce a una repetición automática de la consulta de personalización.
- Un direccionamiento erróneo eventual de los datos de personalización es detectado por el SIM, los datos son desechados y se produce una repetición automática de la consulta de personalización.
- Ante una eventual falta de acuse de recibo del SIM a la red de radiotelefonía móvil, puede producirse automáticamente un nuevo envío de los datos de personalización.

Al proceso de personalización le sigue automáticamente un reinicio en caliente e intento de suscripción con los datos de abonado definitivos. Ahora, en un nuevo proceso por aire se puede realizar, sin presión de tiempo, en el lado de tarjeta una configuración adicional de la relación de abonado.

Ello se refiere a la configuración adicional de la tarjeta SIM con propiedades y servicios especiales, y el chequeo de los datos del cliente y requerimientos de servicios mediante diálogos personales o mecánicos, preferentemente por medio de la terminal de radiotelefonía móvil. Dado el caso, las restricciones de servicio especiales existentes previamente son finalmente eliminadas.

El uso del concepto propuesto no está restringido al canal por aire (que, sin embargo, debería ser el más interesante para la aplicación en redes de radiotelefonía móvil), sino que es posible también en variantes supeditadas a líneas. Por ejemplo, cuando la personalización debe llevarse a cabo de manera descentralizada, pero aún en los puntos de venta (POS) del operador de red o del oferente. Por medio de Internet y un lector de tarjetas conectado, ello es posible, incluso en cualquier lugar. En este caso, los principios, por ejemplo la reutilización del IMS_i^* , son válidos sin cambios, lo mismo que las ventajas a conseguir respecto del estado actual de la técnica. Las siguientes configuraciones ventajosas a modo de ejemplo se detallan en palabras clave:

- todos los sistemas, por ejemplo GSM, UMTS, IMS, WLAN, WIMAX, LTE/SAE/EPS, NGMN, NGN, CDMA
- todas las tarjetas chip de la telecomunicación, por ejemplo UICC, SIM, USIM, ISIM, RUIM y futuras
- todos los factores de forma, por ejemplo ID-1, ID-000, MiniUICC, M2M, IFF y futuros
- todas las formas de realización, por ejemplo borrables, semiborrables y no borrables, soft
- todos los canales por aire, por ejemplo SMS, BIP/CAT-TP, TCP/IP, también RDM
- todos los canales sujetos a líneas, por ejemplo LAN, WAN, Internet
- todos los equipos terminales, por ejemplo teléfonos fijos, móviles, PC y notebooks PC, módulos autónomos de discos
- todos los lectores de tarjetas descentralizados, por ejemplo en POS

- todas las envergaduras, por ejemplo de (IMSI, K) hasta personalizaciones/ individualizaciones completas y descarga de programas
- mit zusätzlicher Absicherung durch PKI-Verfahren, Zertifikate und/oder Personalisierungskennwort
- con derivación de determinados parámetros
- con valoración de la IMEI (personalización específica al equipo)
- con valoración de la ICCID (personalización específica a la tarjeta)
- como servicio por terceros
- como personalización inicial o repersonalización, incluso con cambio de operador de red
- integrado al diálogo on-line, inclusive conclusión de contrato y activación.

Síntesis y/o traducciones de los términos usados y su denominación internacional habitual y abreviatura:

- Teilnehmeridentifizierungsmodul - Módulo de identificación de abonado (Subscriber Identity Modul, SIM)
- Teilnehmeridentifikation - Identificación de abonado (International Mobile Subscriber Identity, IMSI)
- Geräteidentitätsnummer - Número identificador de equipo (International Mobile Equipment Identity, IMEI)
- Mobilfunknummer - Número de radiotelefonía móvil (Mobile Subscriber Integrated Services Digital Network Number, MSISDN)
- Seriennummer des SIM (ICCID) - Número de serie del SIM (ICCID)
- Funkverbindung zur SIM (Over The Air, OTA) - Radiocomunicación al SIM (por aire, OTA)
- Heimatregister bzw. temporäres Heimatregister - Registro de localización geográfica de abonados o registro temporario de localización geográfica de abonados (Home Location Register, HLR o THLR)
- Maschine-Maschine Kommunikation - Comunicación máquina a máquina (machine to machine, M2M)
- Lesen - leer
- Check – comprobación, control, comprobar
- Netzwerk - red
- Anfügen, Angefügt – enexar, anexo
- Zwischenspeichern – almacenamiento temporario
- Authentifizieren, Authentifizierung - autenticación
- Auth. – abreviatura para autenticación
- mangelhaft - deficiente
- Fehler - error
- Senden, übermitteln – enviar, transmitir
- Aktualisierung - actualización
- Generieren - generar
- Sitzung - sesión
- abgesichert - asegurado
- Ausgabe, ausgeben - emisión, emitir
- Personalisierung - personalización
- Personalisierungsprozess – proceso de personalización
- Installieren - instalar
- Ziel, Zielbereich – objetivo, sector de objetivo
- Bestätigung - confirmación
- vollständige Aktualisierung, vollständig aktualisieren – actualización completa, actualizar completamente
- Ack – abreviatura para acuse de recibo
- Zeitüberschreitung - tiempo excedido

REIVINDICACIONES

1. Procedimiento para la puesta en servicio y personalización de módulos de identificación de abonados en una red de radiotelefonía móvil, en el cual un sinnúmero de módulos de identificación de abonados son provistos antes de la primera puesta en servicio de registros paramétricos idénticos, no individuales, no inequívocos provisionales de parámetros iniciales de parámetros de identificación y autenticación, conteniendo al menos una identificación no individual y provisional y una clave secreta no individual y provisional, permitiendo los registros paramétricos la primera puesta en servicio de los módulos de identificación de abonado en la red de radiotelefonía móvil mediante un equipo terminal de radiotelefonía móvil y siendo el número de registros paramétricos menor que el número total de módulos de identificación de abonados equipados con los registros paramétricos de datos, siendo realizada una personalización después de la primera puesta en servicio de uno de los módulos de identificación de abonado transmitiendo un registro de datos de abonado individual y definitivo y siendo almacenado en el módulo de identificación de abonado, conteniendo una identificación de abonado definitiva inequívoca y una clave secreta.

2. Procedimiento según la reivindicación 1, caracterizado por que en la primera puesta en servicio, el establecimiento de una comunicación con un servidor de personalización se produce dentro de la red de radiotelefonía móvil, siendo generado por parte del servidor de personalización el registro de datos de abonado individual y definitivo para la personalización y transmitido al módulo de identificación de abonado, en particular usando el registro de datos de abonado no individuales y provisionales.

3. Procedimiento según las reivindicaciones 1 o 2, caracterizado por que antes de la realización de la personalización se procede a una comprobación de los números de serie del módulo de identificación de abonado y/o el número identificador del equipo mediante el cual el equipo terminal de radiotelefonía es identificable inequívocamente, y/o una comprobación de otros parámetros de seguridad del módulo de identificación de abonado.

4. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que el registro definitivo de abonado es transmitido por medio de una comunicación radiotelefónica por aire del sistema de radiotelefonía móvil usando el registro paramétrico de datos provisional.

5. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que los registros no individuales y provisionales de abonados son reusados cíclicamente en la configuración inicial de los módulos de identificación de abonado, en particular independientemente de si y cuantos de los módulos de identificación de usuarios ya han sido personalizados con registros de datos de abonado individuales y definitivos.

6. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que el registro de datos de abonado generado en la personalización y los datos de abonado correspondientes sólo son almacenados en un registro de localización geográfica de abonados durante la primera puesta en servicio del módulo de identificación de abonado.

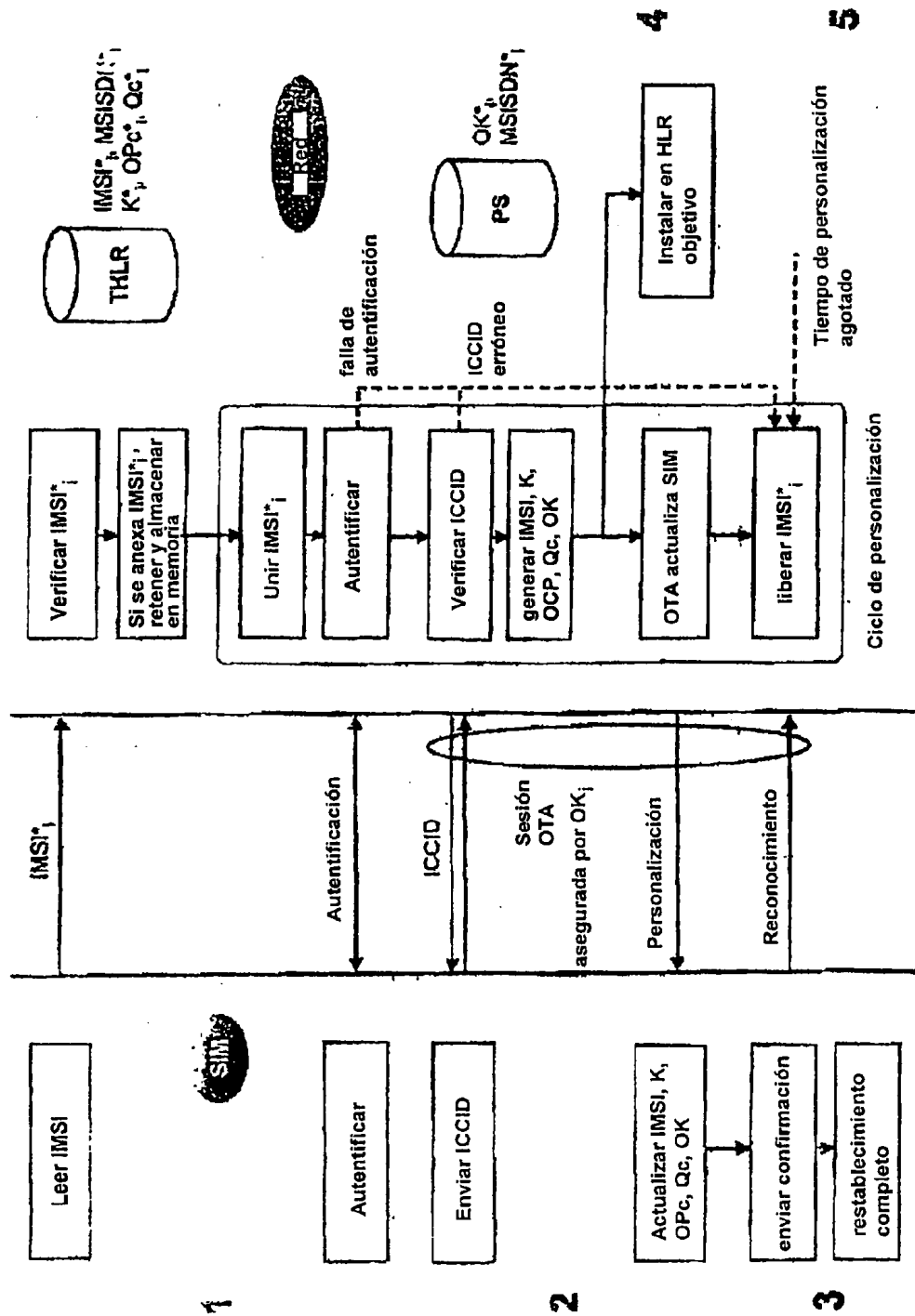
7. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que después de la recepción y el almacenamiento del registro individual y definitivo de abonado en el módulo de identificación de abonado se transmite una confirmación del equipo terminal de radiotelefonía móvil a la red de radiotelefonía móvil, en particular por que se realiza un reinicio en caliente del equipo terminal de radiotelefonía móvil usando el registro de datos de abonado.

8. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que durante la primera puesta en servicio con el registro paramétrico de datos no individual y provisional la condición de abonado proporcionada por la identificación provisional de abonado por el lado de la red es puesta en un estado "en uso", mientras tanto está liberado solamente un uso restringido, y por que después de la personalización realizada del módulo de identificación de abonado mediante el registro de datos de abonado individual y definitivo, la condición de abonado proporcionada por la identificación provisional de abonado es colocada en un estado "liberado" que permite el uso renovado de la condición de abonado proporcionada por la identificación provisional de abonado mediante otro módulo de identificación de abonado.

9. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que en un intento de puesta en servicio de uno o más módulos de identificación de abonados adicionales mediante un primer módulo de identificación de abonado provisional idéntico ya suscrito para la personalización en la red de radiotelefonía móvil, se produce una incorporación a una cola de espera y un procesamiento según el orden cronológico de los intentos de puesta en servicio.

10. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que en un intento de puesta en servicio de uno o más módulos de identificación de usuarios adicionales mediante un primer módulo de identificación de abonado provisional idéntico ya suscrito para la personalización en la red de radiotelefonía móvil, se produce una incorporación a una cola de espera y un procesamiento según el orden cronológico de los intentos de puesta en servicio.

- 5 11. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que en un intento de puesta en servicio de uno o más módulos de identificación de abonados adicionales mediante una identificación de abonado provisional idéntica a un primer módulo de identificación de abonados ya registrado para la personalización en la red de radiotelefonía móvil, el módulo de identificación de abonado detecta un error de direccionamiento eventual de los datos de personalización, los datos son desechados y se produce una repetición automática del requerimiento de personalización.
- 10 12. Procedimiento según la reivindicación 7 o una de las reivindicaciones 8 a 11 relacionadas con la reivindicación 7, caracterizado por que ante la falta la confirmación del terminal de radiotelefonía móvil a la red de radiotelefonía móvil se produce automáticamente un nuevo envío de los datos de personalización.
- 15 13. Procedimiento según las reivindicaciones 6 y 7 o una de las reivindicaciones 8 a 12 relacionadas con las reivindicaciones 6 y 7, caracterizado por que sólo después de la confirmación del terminal de radiotelefonía móvil a la red de radiotelefonía móvil se produce el almacenamiento del registro de datos de abonado definitivo en el registro de localización geográfica de abonados.
- 20 14. Procedimiento según las reivindicaciones 6 y 7 o una de las reivindicaciones 8 a 13 relacionadas con las reivindicaciones 6 y 7, caracterizado por que sólo después de la confirmación del terminal de radiotelefonía móvil a la red de radiotelefonía móvil se produce la activación y/o liberación de la condición de abonado caracterizado mediante el registro de datos de abonado definitivo en el registro de localización geográfica de abonados.
- 25 15. Procedimiento según la reivindicación 6 o una de las reivindicaciones 7 a 14 relacionadas con la reivindicación 6, caracterizado por que los registros de datos de abonado definitivos ya han sido creados previsionalmente en el registro de localización geográfica de abonados.
- 30 16. Procedimiento según la reivindicación 6 o una de las reivindicaciones 7 a 15 relacionadas con la reivindicación 6, caracterizado por que las condiciones de abonados caracterizados mediante los registros de abonado definitivos ya han sido creados previsionalmente en el registro de localización geográfica de abonados.
- 35 17. Procedimiento según la reivindicación 6 o una de las reivindicaciones 7 a 16 relacionadas con la reivindicación 6, caracterizado por que las condiciones de abonados ya han sido creados previsionalmente en el registro de localización geográfica de abonados con restricciones de servicios específicos.
- 40 18. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que a continuación de la personalización se producen automáticamente procesos de carga adicionales para la configuración del módulo de identificación de abonado con propiedades y/o servicios particulares.
19. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que a continuación de la personalización realizada se inicia automáticamente con el cliente un diálogo mecánico o personal a través de la terminal de radiotelefonía móvil para el chequeo de datos del cliente y/o requerimientos de servicios.



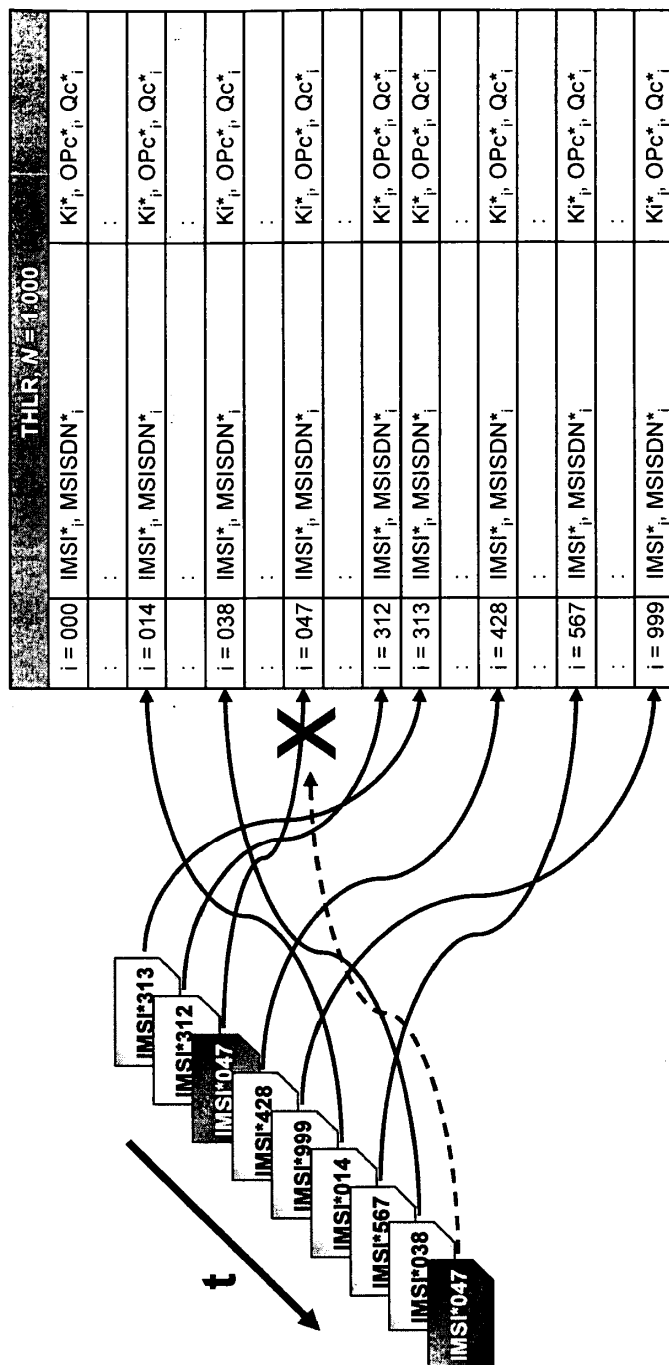


Fig. 2