(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 782 835**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04W 8/20 (2009.01)
H04W 4/14 (2009.01)
H04L 12/24 (2006.01)
H04W 4/50 (2008.01)
H04W 4/60 (2008.01)
H04W 12/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **21.11.2014 PCT/FR2014/052989**

(87) Fecha y número de publicación internacional: **28.05.2015 WO15075395**

(96) Fecha de presentación y número de la solicitud europea: **21.11.2014 E 14821726 (8)**

(97) Fecha y número de publicación de la concesión europea: **01.01.2020 EP 3072322**

(54) Título: **Método de notificación para configurar un elemento seguro**

(30) Prioridad:

21.11.2013 FR 1361481

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.09.2020

(73) Titular/es:

IDEMIA FRANCE (100.0%)
420, rue d'Estienne d'Orves
92700 Colombes, FR

(72) Inventor/es:

DANREE, ARNAUD y
LARIGNON, GUILLAUME

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método de notificación para configurar un elemento seguro

ANTECEDENTES DE LA INVENCIÓN

La presente invención se refiere al campo de la configuración de un elemento seguro incorporado en un terminal.

La invención se aplica en particular, y de forma no limitativa, a los elementos seguros de tipo "UICC" (Tarjeta de Circuito Integrado Universal) ("Universal Integrated Circuit Card" en terminología inglesa) y "eUICC" (Tarjeta de Circuito Integrado Universal integrada) ("embedded Universal Integrated Circuit Card" en terminología inglesa).

Para obtener más información sobre los elementos seguros "UICC" y "eUICC", los expertos en esta técnica consultarán, respectivamente, la norma "ETSI 102.221" y las especificaciones "ETSI TS 103 383".

En el presente documento, el concepto de "perfil de personalización" debe interpretarse en sentido amplio, es decir, como un conjunto de al menos un fichero y/o datos. Un perfil de personalización, en el sentido de la invención, puede comprender en particular al menos un elemento entre:

- un fichero patrón tal como se define por las especificaciones 3GPP o ETSI para los UICC y sus aplicaciones y, en particular, por las normas 3GPP 31.102 y ETSI 102.221;
- un fichero propietario;
- un fichero de configuración de un sistema operativo;
- una aplicación Java Card y elementos de personalización asociados;
- datos tales como claves de protocolo de transporte, parámetros del algoritmo de autenticación, ...

El perfil de personalización se utiliza por una aplicación comercial para comunicarse con entidades externas al terminal.

De manera conocida, cuando un operador desea instalar un nuevo perfil de personalización en un elemento seguro, este operador utiliza un módulo de configuración de un servidor distante. Este módulo de configuración es capaz de enviar datos al elemento seguro según un protocolo de transporte seguro, siendo la seguridad de los intercambios realizada por medio de una clave compartida por estas dos entidades. De este modo, el operador envía datos que comprenden un script para instalar el perfil, que a continuación se ejecuta con el fin de instalar el perfil en el elemento seguro.

Sin embargo, el perfil cargado, elegido por el operador, no siempre es el perfil que permite utilizar el terminal de forma óptima.

Uno de los objetivos de la invención es resolver dicho problema.

Más en general, la invención se refiere a mecanismos para facilitar la configuración de un elemento seguro incorporado en un terminal.

El documento EP 1 530 392 describe un método de gestión de la seguridad de aplicaciones con un módulo de seguridad. El documento US 2011/0136482 describe un método para personalizar una tarjeta de circuito integrado. El documento US 2012/0036282 describe un método para configurar una tarjeta de circuito integrado.

SUMARIO DE LA INVENCIÓN

La presente invención se define en las reivindicaciones independientes. Las reivindicaciones dependientes definen formas de realización preferidas.

A este efecto, la presente invención se refiere a un método de notificación con el fin de configurar un elemento seguro incorporado en un terminal conectado a una red, cuyo método comprende las etapas siguientes puestas en práctica por una aplicación del elemento seguro:

- obtener al menos un elemento de información útil para la configuración del elemento seguro almacenado en una memoria del terminal externo al elemento seguro,
- enviar el elemento de información y un identificador del elemento seguro a un sistema de configuración, y

- obtener datos de configuración procedentes del sistema de configuración, siendo dichos datos de configuración suministrados al elemento seguro en función del elemento de información.

La invención es ventajosa por cuanto que los datos de configuración se suministran en función del elemento de información útil para la configuración del elemento seguro. Por lo tanto, el envío del elemento de información hace posible elegir los datos de configuración más adecuados para el elemento seguro incorporado en el terminal. Además, enviar el elemento de información le permite elegir cómo enviar los datos de configuración más adecuados. Estos métodos son, por ejemplo, el instante de envío de los datos de configuración, y/o la red utilizada para este envío.

En una forma de realización particular, la aplicación se ejecuta por un sistema operativo del elemento seguro.

En una forma de realización particular, las etapas para obtener el elemento de información y enviar el elemento de información y un identificador del elemento seguro se ponen en práctica durante una puesta bajo tensión del elemento seguro y/o de forma periódica.

La puesta en práctica de estas etapas cuando el elemento seguro se pone bajo tensión permite configurar el terminal tan pronto como se conecta a una red por primera vez.

La puesta en práctica periódica de estas etapas permite que los datos de configuración se actualicen en caso de un cambio en el uso del terminal y/o en caso de un cambio en la red utilizada por el terminal.

En una forma de realización particular, el envío del elemento de información y el identificador del elemento seguro se realiza según la instrucción de control Sim Tool Kit "ENVIAR SMS" o "ABRIR CANAL", definida por la norma "3GPP 31.111". La instrucción de control "ABRIL CANAL" es una instrucción de control proactiva que permite que el elemento seguro y el terminal se comuniquen.

En general, el elemento seguro puede obtener el elemento de información por cualquier medio, bien sea directamente por el módulo terminal que comprende el elemento de información, bien sea por un módulo que se encarga de obtener y luego enviar el elemento de información, estando este elemento de información contenido en otro módulo del terminal. En particular, el elemento seguro puede obtener el elemento de información desde una interfaz de comunicación del terminal con la red, o desde una aplicación ejecutada por un procesador del terminal, siendo esta aplicación externa al elemento seguro. La interfaz de comunicación del terminal con la red es, por ejemplo, un módulo de radio o un módulo de acceso a una red de Internet o telefónica.

En una forma de realización particular, el elemento de información se obtiene a petición de la aplicación del elemento seguro. Esta demanda puede enviarse a la interfaz de comunicación o a la aplicación ejecutada por el procesador del terminal. Esta demanda puede estar conforme con la instrucción de control "PROPORCIONAR INFORMACIÓN LOCAL" del Sim Tool Kit definido por la norma "3GPP 31.111".

En una forma de realización particular, el terminal realiza las siguientes etapas:

- envío de una demanda para leer el elemento de información mediante la interfaz de comunicación a la aplicación ejecutada por el procesador del terminal, y

- envío del elemento de información por la aplicación ejecutada por el procesador del terminal a la interfaz de comunicación,

  o

- envío de una demanda para leer el elemento de información por la aplicación ejecutada por el procesador del terminal en la interfaz de comunicación, y

- envío del elemento de información a través de la interfaz de comunicación a la aplicación ejecutada por el procesador del terminal.

En una forma de realización particular, las diferentes etapas del método de notificación están determinadas por instrucciones de programas de ordenador.

En consecuencia, la invención también se refiere a un primer programa de ordenador en un medio de información (o medio de registro), siendo este primer programa capaz de ponerse en práctica en un elemento seguro o más en general en un ordenador y posiblemente un segundo programa de ordenador en un medio de información capaz de ponerse en práctica en un terminal o, más en general, en un ordenador, incluyendo estos programas instrucciones adaptadas a la puesta en práctica de las etapas de un método de notificación tal como se definió con anterioridad.

Estos programas pueden utilizar cualquier lenguaje de programación y tener la forma de código fuente, código objeto o código intermedio entre el código fuente y el código objeto, tal como en una forma particularmente compilada o en

cualquier otra forma deseable.

La invención también se refiere a un primer medio de información (o medio de registro) legible por un elemento seguro o más en general por un ordenador, y que comprende instrucciones de un primer programa informático tal como se mencionó con anterioridad.

La invención también se refiere a un segundo medio de información (o medio de registro) legible por un terminal o más en general por un ordenador, y que comprende instrucciones de un segundo programa de ordenador tal como se mencionó con anterioridad.

Los medios de información pueden ser cualquier entidad o dispositivo capaz de memorizar los programas. Por ejemplo, los medios pueden incluir un medio de almacenamiento, tal como una memoria no volátil regrabable (del tipo “EEPROM” o “Flash NAND”, por ejemplo), o como una memoria “ROM”, por ejemplo, un “CD ROM” o una memoria “ROM” de circuito microelectrónico, o bien un medio de registro magnético, por ejemplo, un disquete (“floppy disc”) o un disco duro.

Por otro lado, los medios de información pueden ser medios transmisibles, tales como señales eléctricas u ópticas, que pueden enrutarse a través de cables eléctricos u ópticos, por radio o por otros medios. Los programas según la invención se pueden descargar en particular de una red del tipo Internet.

De manera alternativa, los medios de información pueden ser circuitos integrados en los que se incorporan los programas, adaptándose los circuitos para ejecutar o para ser utilizados en la ejecución del método en cuestión.

La invención se refiere, además, a un elemento seguro destinado a ser incorporado en un terminal conectado a una red, comprendiendo dicho elemento seguro una aplicación que incluye:

- medios para obtener al menos un elemento de información útil para la configuración del elemento seguro almacenado en una memoria del terminal externo al elemento seguro,
- medios para enviar dicho elemento de información y un identificador del elemento seguro a un sistema de configuración, y
- medios para obtener datos de configuración procedentes del sistema de configuración, siendo dichos datos de configuración suministrados al elemento seguro en función de dicho elemento de información.

En una forma de realización particular, el elemento seguro cumple con la norma "ISO 7816" y puede procesar instrucciones de control del tipo "APDU".

En una forma de realización particular, el elemento seguro es del tipo "UICC" o del tipo "eUICC".

En una forma de realización particular, la aplicación del elemento seguro es ejecutada por un sistema operativo del elemento seguro.

La invención se refiere, además, a un terminal que comprende un elemento seguro tal como se definió con anterioridad.

La invención se refiere, además, a un método para configurar un elemento seguro incorporado en un terminal conectado a una red, siendo el método puesto en práctica mediante un sistema de configuración, cuyo método comprende:

- obtener y memorizar al menos un elemento de información útil para la configuración del elemento seguro y un identificador del elemento seguro que se origina en el elemento seguro,
- establecer un canal de comunicación seguro con el elemento seguro, y
- enviar los datos de configuración al elemento seguro a través del canal de comunicación, siendo suministrados los datos de configuración al elemento seguro en función de dicho elemento de información.

En una forma de realización particular, los datos de configuración son datos de personalización.

En una forma de realización particular, el envío de los datos de configuración se realiza según un protocolo que comprende una etapa de cifrado y/o firma.

En una forma de realización particular, el protocolo es uno de entre:

- el "Protocolo de Canal Seguro 80",

- el "Protocolo de Canal Seguro 81",
- el "Protocolo de Canal Seguro 02", y
- el "Protocolo de Canal Seguro 03",

definidos por la norma "Global Plateform 2.2".

En una forma de realización particular, el elemento de información es uno de entre:

- el número "IMEI" del terminal,
- el número "IMEISV" del terminal,
- el país en donde se encuentra el terminal,
- dicha red,
- la potencia de dicha red,
- el tipo de canal de comunicación soportado por el terminal, y
- el tipo de portadora utilizado por el terminal.

En una forma de realización particular, el identificador del elemento seguro es uno de entre:

- el "ID de eUICC" definido por la versión 1.46 de la especificación de "Arquitectura de aprovisionamiento distante para UICC incorporada" de la "Global System for Mobile Communications Association" (Asociación del Sistema Global para Comunicaciones Móviles",
- la "ID de ICC" definida por la norma "ISO 7812", y
- el "IMSI".

En una forma de realización particular, los métodos de envío de datos de configuración se eligen en función con el elemento de información.

En una forma de realización particular, el elemento de información se utiliza para determinar al menos uno de los elementos entre:

- la red utilizada para enviar los datos de configuración,
- el canal de comunicación utilizado para enviar los datos de configuración,
- la portadora utilizada para enviar los datos de configuración.

De manera más general, el elemento de información puede utilizarse, por ejemplo, para determinar al menos uno los elementos entre:

- un perfil de personalización adaptado al tipo de terminal,
- un perfil de personalización adaptado al país en donde se encuentra el terminal,
- el momento de enviar datos de configuración,
- la red utilizada para enviar los datos de configuración,
- el canal de comunicación utilizado para enviar los datos de configuración,
- la portadora utilizada para enviar los datos de configuración.

La determinación de un perfil de personalización adaptado al tipo de terminal puede realizarse cuando el elemento de información es el número "IMEI" o "IMEISV" del terminal. La determinación de un perfil de personalización adaptado al país en donde se encuentra el terminal se puede realizar cuando el elemento de información es el código "MCC" del terminal. Los datos de configuración son, entonces, datos de personalización que comprenden un script para instalar el perfil.

Además, la determinación del instante de envío de los datos de configuración se puede realizar cuando el elemento de información es el código "NMR". El módulo de configuración a continuación envía los datos de configuración cuando la cobertura de la red es de buena calidad. Además, la red utilizada para enviar los datos de configuración se puede determinar cuando el elemento de información es el código "MNC". Además, la determinación del canal de comunicación utilizado para enviar los datos de configuración puede realizarse cuando el elemento de información indica los diferentes tipos de canales de comunicación soportados por el terminal y la determinación de la portadora puede realizarse cuando el elemento de información indica el tipo de portadora que puede utilizar el terminal.

En una forma de realización particular, el método comprende la determinación (por el sistema de configuración), a partir de dicho al menos un elemento de información, del canal de comunicación de mayor velocidad soportado por el elemento seguro (o a través del terminal),

dicho canal de comunicación de mayor velocidad se utiliza como un canal de comunicación seguro durante la etapa de enviar datos de configuración al elemento seguro.

En una forma de realización particular, el método comprende una etapa de verificación (por el sistema de configuración) para verificar si un canal de comunicación cuya velocidad de bits es al menos igual a un valor umbral predeterminado puede establecerse con el elemento seguro (o más en general con el terminal) o para verificar si se puede establecer un canal de comunicación de un tipo predeterminado con el elemento seguro (o más en general con el terminal), y:

- en caso afirmativo, el envío de los primeros datos como datos de configuración durante la etapa de envío al elemento seguro;

- en caso negativo, el envío de segundos datos como datos de configuración durante la etapa de envío al elemento seguro, en donde los primeros datos son de magnitud (en términos de espacio de memoria) mayor que los segundos datos.

Los primeros datos y los segundos datos son, por ejemplo, perfiles de personalización.

El sistema de configuración puede así adaptar los datos de configuración que envía al elemento seguro en función con el tipo de canal de comunicación (o el protocolo de comunicación) soportado por el elemento seguro (o más en general por el terminal en donde se incorpora dicho elemento seguro).

En un ejemplo particular, el tipo predeterminado es el tipo "https". Dicho de otro modo, durante la etapa de verificación, el sistema de configuración verifica si se puede establecer un canal de comunicación del tipo https (o según el protocolo https) con el elemento seguro (o más en general con el terminal). En este caso, los primeros datos están, por ejemplo, adaptados para ser enviados según el protocolo https. Además, los segundos datos están, por ejemplo, adaptados para ser transmitidos al elemento seguro según el protocolo SMS.

Por lo tanto, es posible optimizar la transmisión de datos de configuración al elemento seguro.

Los primeros datos son, por ejemplo, 2, 5, 10 o incluso 20 veces más grandes en términos de magnitud de datos que los segundos datos. Dicho de otro modo, los primeros datos tienen una magnitud de datos N veces mayor que los segundos datos, siendo N igual a uno de entre los valores 2, 5, 10 y 20.

En una forma de realización particular, el sistema de configuración determina, a partir de dicho al menos un elemento de información, el tipo de terminal en donde se incorpora el elemento seguro. El terminal puede ser, por ejemplo, un teléfono móvil (o más en general un terminal de telecomunicaciones móvil) o un medidor eléctrico, tal como se explica con más detalle en el resto de este documento. Dependiendo del tipo de terminal así determinado, el sistema de configuración puede determinar al menos uno de los siguientes parámetros:

(a) los datos de configuración que se enviarán al elemento seguro durante dicha etapa de envío (seleccionando, por ejemplo, los primeros datos o los segundos datos mencionados con anterioridad);

(b) el canal de comunicación, el protocolo de comunicación y/o la portadora que se utilizará durante dicha etapa de enviar datos de configuración al elemento seguro.

En una forma de realización particular, las diferentes etapas del método de configuración están determinados por instrucciones de programas de ordenador.

En consecuencia, la invención también se refiere a un programa de ordenador en un medio de información (o medio de registro), siendo este programa susceptible de ponerse en práctica por un sistema de configuración o más en general en un ordenador, incluyendo este programa instrucciones adaptadas a la puesta en práctica de las etapas de un método de configuración tal como se definió con anterioridad.

Este programa puede utilizar cualquier lenguaje de programación y tener la forma de código fuente, código objeto o código intermedio entre el código fuente y el código objeto, tal como en una forma particularmente compilada o en cualquier otra forma deseable.

La invención también se refiere a un medio de información (o medio de registro) legible por un sistema de configuración o más en general por un ordenador, y que comprende instrucciones de un programa informático tal como se mencionó con anterioridad.

El medio de información puede ser cualquier entidad o dispositivo capaz de memorizar el programa. Por ejemplo, el medio puede incluir un medio de almacenamiento, tal como una memoria no volátil regrabable (del tipo “EEPROM” o “Flash NAND”, por ejemplo), o como una memoria “ROM”, por ejemplo, un “CD ROM o una memoria “ROM” de circuito microelectrónico, o también un medio de registro magnético, por ejemplo, un disquete (“floppy disc”) o un disco duro.

Por otro lado, el medio de información puede ser un medio transmisible, tal como una señal eléctrica u óptica, que puede enrutarse a través de un cable eléctrico u óptico, por radio o por otros medios. El programa según la invención se puede descargar en particular de una red del tipo Internet.

De manera alternativa, el medio de información puede ser un circuito integrado en donde se incorpora el programa, adaptándose el circuito para ejecutar o para ser utilizado en la ejecución del método en cuestión.

La invención se refiere, además, a un sistema de configuración para un elemento seguro incorporado en un terminal conectado a una red, comprendiendo el sistema de configuración:

- un módulo de gestión capaz de obtener al menos un elemento de información útil para la configuración del elemento seguro y un identificador del elemento seguro procedente del elemento seguro,
- un módulo de comunicación seguro con el elemento seguro, pudiendo el módulo de comunicación seguro establecer un canal de comunicación seguro con el elemento seguro,
- una primera memoria capaz de memorizar el elemento de información y el identificador del elemento seguro, y
- un módulo de configuración capaz de enviar datos de configuración al elemento seguro a través del canal de comunicación, siendo suministrados los datos de configuración al elemento seguro en función del elemento de información.

En una forma de realización particular, el módulo de comunicación segura comprende medios de descifrado.

En una forma de realización particular, el módulo de configuración comprende:

- medios para enviar el identificador del elemento seguro a la primera memoria, y
- medios de recuperación, en respuesta al envío, del elemento de información.

En una forma de realización particular, el módulo de configuración comprende:

- medios para enviar el elemento de información a una segunda memoria, y
- medios de recuperación, en respuesta a dicho envío de los datos de configuración.

Además, la invención se refiere a un sistema que comprende un terminal que incluye un elemento seguro tal como se definió con anterioridad, siendo este terminal y este elemento seguro capaces de poner en práctica un método de notificación tal como se definió con anterioridad, y un sistema de configuración tal como se definió con anterioridad, siendo este sistema de configuración capaz de poner en práctica un método de configuración tal como se definió con anterioridad.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Otras características y ventajas de la presente invención surgirán de la descripción proporcionada a continuación, con referencia a los dibujos adjuntos que ilustran un ejemplo de realización desprovisto de cualquier carácter limitativo. En las figuras:

La Figura 1 representa, de manera esquemática, las arquitecturas de hardware de un terminal, de un elemento seguro y de un sistema de configuración de conformidad con una forma de realización de la invención;

La Figura 2 representa en particular, en forma de diagrama de flujo, las etapas principales de un método de notificación

y de un método de configuración de conformidad con una forma de realización de la invención.

DESCRIPCIÓN DETALLADA DE VARIAS FORMAS DE REALIZACIÓN

La presente invención se refiere al campo de la configuración de un elemento seguro incorporado en un terminal y se refiere, más en particular, a la configuración de dicho elemento seguro por un sistema de configuración a partir de elementos de información transmitidos por el elemento seguro a este sistema de configuración.

La Figura 1 muestra, de manera esquemática y según una primera forma de realización, un elemento seguro 100 incorporado en un terminal 120 configurado para poder cooperar, a través de una red 140, con un sistema de configuración 160.

El elemento seguro 100 es, en un ejemplo, de conformidad con la norma "ISO 7816" y capaz de procesar instrucciones de control del tipo "APDU" (Unidad de Datos del Protocolo de Aplicación) ("Application Protocol Data Unit" en terminología inglesa). Por lo tanto, este elemento seguro 100 puede ser del tipo "UICC" (Tarjeta de Circuito Integrado Universal) ("Universal Integrated Circuit Card" en terminología inglesa). Como variante, el elemento seguro puede ser del tipo "eUICC" (Tarjeta de Circuito Integrado Universal integrada) ("embedded Universal Integrated Circuit Card" en terminología inglesa). Además, el terminal 120 puede ser, por ejemplo, un teléfono móvil, un automóvil, una lavadora, una farola o un medidor eléctrico. Además, la red 140 puede ser, por ejemplo, una red de Internet o una red telefónica.

El elemento seguro 100 tiene la arquitectura convencional de un ordenador. Este elemento seguro 100 incluye, en particular, un procesador 101, un sistema operativo 102, una memoria de solo lectura 103 (del tipo "ROM"), una memoria no volátil regrabable 104 (del tipo "EEPROM" o "Flash NAND", por ejemplo), una memoria volátil regrabable 105 (del tipo "RAM") y una interfaz de comunicación 106.

En este ejemplo, la memoria de solo lectura 103 constituye un medio de información (o registro) de conformidad con una forma de realización particular de la invención. En la memoria de solo lectura 103 se almacena un primer programa informático P1 que permite que el elemento seguro ponga en práctica una primera parte del método de notificación de conformidad con una forma de realización particular de la invención (véase la Figura 2). Como variante, el primer programa informático P1 se almacena en la memoria no volátil regrabable 104.

Además, la memoria de solo lectura 103 almacena una aplicación 108 puesta en práctica por el sistema operativo 102. Como variante, la aplicación 108 se almacena en la memoria no volátil regrabable 104. Como otra variante, la aplicación 108 es almacenada en el sistema operativo 102.

El terminal 120 también tiene la arquitectura convencional de un ordenador. Dicho terminal 120 comprende, en particular, un procesador 121, una memoria de solo lectura 122 (del tipo "ROM"), una memoria no volátil regrabable 123 (del tipo "EEPROM" o "flash NAND", por ejemplo), una memoria volátil regrabable 124 (del tipo "RAM"), y una interfaz de comunicación 125 con la red 140 y con la interfaz de comunicación 106 del elemento seguro 100.

En este ejemplo, la memoria de solo lectura 122 constituye un medio de información (o registro) de conformidad con una forma de realización particular de la invención. En la memoria de solo lectura 122 se almacena un segundo programa informático P2 que permite que el terminal 120 ponga en práctica una segunda parte del método de notificación de conformidad con una forma de realización particular de la invención (véase Figura 2). Como variante, el segundo programa informático P2 se almacena en la memoria no volátil regrabable 123.

Además, la memoria de solo lectura 122 almacena una aplicación 126 ejecutada por el procesador 121. Como variante, la aplicación 126 se almacena en la memoria no volátil regrabable 123.

En un ejemplo, una memoria de la interfaz de comunicación 125 almacena un primer elemento de información 128 útil para la configuración del elemento seguro 100. Además, en este ejemplo, la aplicación 126 almacena un segundo elemento 129 útil para la configuración del elemento seguro 100.

El sistema de configuración 160 comprende un módulo de gestión 161, un módulo de configuración 162, una primera memoria 163, una segunda memoria 164 y un módulo de comunicación segura 165 con el elemento seguro 100. Además, el sistema de configuración 160 almacena un programa P3. En un ejemplo, el sistema de configuración 160 está incluido en un servidor distante que presenta la arquitectura convencional de un ordenador. En otro ejemplo, los módulos 161, 162, 165 y las memorias 163, 164 del sistema de configuración se distribuyen en varios servidores distantes, presentando cada uno de estos servidores la arquitectura convencional de un ordenador. En este caso, los servidores distantes se comunican entre sí por medio de una red de comunicación posiblemente segura.

La Figura 2 muestra, todavía según la primera forma de realización, un método de notificación con el fin de configurar el elemento seguro 100. Se ponen en práctica las etapas A200, A215, A220, A275 de este método de notificación mediante la aplicación 108 del elemento seguro 100 que ejecuta el programa P1 y las etapas B200, B205, C205, B210, C210 y B215 de este método de notificación son puestas en práctica por el terminal 120 que ejecuta el programa P2.

En una etapa A200, la aplicación 108 envía una demanda M200 para leer el primer elemento de información 128 útil para la configuración del elemento seguro 100 a una interfaz de comunicación 125 del terminal 120. Al recibir esta demanda M200, la interfaz de comunicación 125 envía (B215) el primer elemento de información 128 a la aplicación 108.

Como variante, la aplicación 108 envía una demanda M200 para leer el segundo elemento de información 129 útil para la configuración del elemento seguro 100. En esta variante, la interfaz de comunicación 125 del terminal 120 envía entonces, en una etapa B205, una demanda M205 para leer el segundo elemento de información 129 a la aplicación 126 del terminal 120. Al recibir dicha demanda, la aplicación 126 envía (C210) a la interfaz de comunicación 125 el segundo elemento de información 129. A continuación, la interfaz de comunicación 125 envía (B215) el segundo elemento de información 129 a la aplicación 108.

Como variante, la aplicación 108 envía una demanda M200 para leer el primer elemento de información 128 y el segundo elemento de información 129. En esta variante, la interfaz de comunicación 125 del terminal 120 envía, en una etapa B205, una demanda M205 para leer el segundo elemento de información 129 a la aplicación 126 del terminal 120. Al recibir dicha demanda, la aplicación 126 envía (C210) a la interfaz de comunicación 125 el segundo elemento 129. A continuación, la interfaz de comunicación 125 envía (B215) el primer elemento de información 128 y el segundo elemento de información 129 a la aplicación 108.

En una segunda forma de realización, la interfaz de comunicación 106 del elemento seguro 100 no se comunica con la interfaz de comunicación 125 y se comunica con la aplicación 126. Esta segunda forma de realización es una variante de la primera la forma de realización descrita con anterioridad y difiere solamente en que el terminal 120 tiene otra configuración lógica o de hardware, lo que tiene la consecuencia de que la aplicación 108 del elemento seguro 100 se comunica con la aplicación 126 en lugar de comunicarse con la interfaz de comunicación 125. Por lo tanto, en esta forma de realización, la aplicación 108 envía (A200) una demanda M200 para leer el segundo elemento de información 129 a la aplicación 126. Al recibir esta demanda M200, la aplicación 126 envía (B215) el segundo elemento de información 129 a la aplicación 108. Como variante, la aplicación 108 envía una demanda M200 para leer el primer elemento de información 128 a la aplicación 126. En esta variante, la aplicación 126 envía, en una etapa B205, una demanda M205 para leer el primer elemento de información 128 a la interfaz de comunicación 125 del terminal 120. Al recibir dicha demanda, la interfaz de comunicación 125 envía (C210) a la aplicación 126 el primer elemento de información 128. A continuación, la aplicación 126 envía (B215) el primer elemento de información 128 a la aplicación 108. Como variante, la aplicación 108 envía una demanda M200 para leer el primer elemento de información 128 y el segundo elemento de información 129 a la aplicación 126. En esta variante, la aplicación 126 envía, en una etapa B205, una demanda M205 para lectura del primer elemento de información 128 a la interfaz de comunicación 125 del terminal 120. Al recibir dicha demanda, la interfaz de comunicación 125 envía (C210) a la aplicación 126 el primer elemento de información 128. A continuación, la aplicación 126 envía (B215) el primer elemento de información 128 y el segundo elemento de información 129 a la aplicación 108.

En ambas formas de realización, los envíos de demandas y datos entre la interfaz de comunicación 125 y la aplicación 126 del terminal 100 se lleva a cabo, por ejemplo, de conformidad con las instrucciones de control "AT" definidas por la norma "3GPP TS 27.007"

Además, la demanda M200 enviada por la aplicación 108 puede estar de conformidad con la instrucción de control "Sim Tool Kit PROPORCIONAR INFORMACIÓN LOCAL" definida por la norma "3GPP 31.111".

La aplicación 108 envía la demanda M200 cuando se pone bajo tensión el elemento seguro 100. Como variante, la aplicación 108 envía la demanda M200 de manera periódica. En otra variante, la aplicación 108 envía la demanda M200 cuando el elemento seguro 100 se activa y de manera periódica.

Como variante, la etapa A200 no se realiza y la interfaz de comunicación 125 (o la aplicación 126) envía (B215) el elemento de información 128 y/o 129 a la aplicación 108, cuando el elemento seguro 100 se activa y/o de manera periódica, según una instrucción de control "APDU" definida por la norma "ISO 7816", o también según una instrucción de control "PERFIL DEL TERMINAL" definida por la norma "3GPP TS 31.111".

Cuando se obtiene el elemento de información 128 y/o 129 (A215) después de una demanda M200 enviada de conformidad con la instrucción de control “Sim Tool Kit PROPORCIONAR INFORMACIÓN LOCAL” definida por la norma “3GPP 31.111”, este elemento de información 128 y/o 129 es el número "IMEI" (Identidad Internacional de Equipo Móvil) ("International Mobile Equipment Identity" en terminología inglesa), o el número "IMEISV" (Versión de Software de Identidad Internacional de Equipo Móvil) (“International Mobile Equipment Identity Software Version” en terminología inglesa), o el código "MCC" (Código de País Móvil) (“Mobile Country Code" en terminología en inglesa), o el código "MNC" (Código de Red Móvil) (“Mobile Network Code” en terminología inglesa), o el código "NMR" (Informe de Medición de Red) (“Network Mesurement Report" en terminología inglesa). De manera alternativa, este elemento de información 128 y/o 129 es una combinación de los números y códigos mencionados con anterioridad. Los números "IMEI" e "IMEISV", así como los códigos "MCC", "MNC" y "NMR" están definidos, por ejemplo, en la especificación "3GPP TS 31.111". Los números "IMEI" e "IMEISV" son identificadores del terminal 120. Los números "IMEI" e "IMEISV" incluyen un número "TAC" (Código de Asignación de Tipo) (Type Allocation Code” en terminología inglesa)

que define el país donde el terminal 120 se ha registrado, un número de "SNR" (Número de Serie) ("Serial Number" en terminología inglesa) correspondiente al número de serie y una suma de control. El código "MCC" corresponde al país en donde se encuentra el terminal 120. El código "MNC" define la red 140. Además, el código "NMR" indica la potencia de la red 140.

En una puesta en práctica particular, el elemento de información 128 y/o 129 indica (en el byte 17 de una instrucción de control "PERFIL DE TERMINAL" por ejemplo) los diferentes tipos de canales de comunicación soportados por el terminal 120, por ejemplo, para el protocolo "BIP" (Protocolo Independiente del Portador) ("Beaver Independant Protocol" en terminología inglesa) cuando se obtiene el elemento de información 128 y/o 129 (A215) gracias a una instrucción de control "PERFIL DEL TERMINAL" definida por la norma "3GPP TS 31.111".

En una puesta en práctica particular, el elemento de información 128 y/o 129 indica (por ejemplo, el byte 13 de una instrucción de control "PERFIL DEL TERMINAL") el tipo de portadora que puede utilizar el terminal 120. Esta portadora es, por ejemplo, del tipo "CSD" (Datos de Circuitos Conmutados) ("Circuit Switched Data" en terminología inglesa), "GPRS" (Servicio General de Radio por Paquetes) ("General Packet Radio Service" en terminología inglesa), "Bluetooth", "IrDA" (Asociación de Datos Infrarrojos) (Infrared Data Association" en terminología inglesa) o "RS 232".

A continuación, en una etapa A220, la aplicación 108 del elemento seguro 100 envía el elemento de información 128 y/o 129 y un identificador ID del elemento seguro 100 al módulo de gestión 161 del sistema de configuración 160. En un ejemplo, este envío se realiza de conformidad con la instrucción de control Sim Tool Kit "ENVIAR SMS" o "ABRIR CANAL", definida por la norma "3GPP 31.111". La instrucción de control "ABRIL CANAL" es una instrucción de control proactiva que permite que el elemento seguro y el terminal se comuniquen.

El identificador ID del elemento seguro 100 es, en un ejemplo, el "ID de eUICC" definido por la versión 1.46 de la especificación de "Arquitectura de aprovisionamiento distante para UICC integrado" del "Sistema global para la Asociación de Comunicaciones Móviles" el "ID de ICC" definido por la norma "ISO 7812", o el "IMSI" (Identidad Interna de Abonado Móvil" ("Internal Mobile Subscribe Identity" en terminología inglesa).

En el caso en que se utiliza la instrucción de control Sim Tool Kit "ENVIAR SMS", no es necesario enviar el identificador ID del elemento seguro 100, ya que el encabezado del mensaje enviado por esta instrucción de control comprende el "IMSI". De hecho, la red 140 conoce el "IMSI" del terminal 120 cuando este terminal 120 está conectado a dicha red 140.

Además, como se da a conocer con más detalle a continuación, la aplicación 108 del elemento seguro 100 obtiene, en una etapa A275, a través de un canal de comunicación seguro, datos de configuración de CC procedentes del módulo de configuración 162 del sistema de configuración 160, siendo estos datos de configuración DC suministrados al elemento seguro 100 en función del elemento de información 128 y/o 129.

La Figura 2 representa, según una forma de realización, un método para configurar el elemento seguro 100, puesto en práctica por el sistema de configuración 160 que ejecuta el programa P3.

Este método comprende una etapa D220 para obtener, mediante el módulo de gestión 161, el elemento de información 128 y/o 129 y el identificador IDE del elemento seguro 100 enviado por la aplicación 108 del elemento seguro 100. Este método comprende, además, una etapa D225 de establecimiento de un canal de comunicación CN seguro con el elemento seguro 100.

A continuación, en una etapa D230, el módulo de gestión 161 memoriza el elemento de información 128 y/o 129 y el identificador ID del elemento seguro 100 en la primera memoria 163.

Al configurar el elemento seguro 100, el módulo de personalización 162 envía, en una etapa E250, el identificador ID del elemento seguro 100 a la primera memoria 163.

La etapa E250 se lleva a cabo, por ejemplo, después de la primera memorización (D230) del elemento de información 128 y/o 129 y el identificador ID del elemento seguro 100 por el módulo de gestión 161 en la primera memoria 163. En otro ejemplo, la etapa E250 se lleva a cabo periódicamente. En otro ejemplo, la etapa E250 se realiza después de la primera memorización (D230) y periódicamente.

En respuesta a este envío de la etapa E250, el elemento de información 128 y/o 129 es recuperado (E255) por el módulo de personalización 162. A continuación, el módulo de personalización 162 envía, en una etapa E260, el elemento de información 128 y/o 129 a la segunda memoria 164. En respuesta a este envío, el módulo de personalización 162 recupera los datos de configuración DC del elemento seguro 100 (E265).

La etapa E265 es seguida por una etapa E275 de envío de datos de configuración DC por el módulo de configuración 162 a la aplicación 108 del elemento seguro 100 a través del canal de comunicación CN.

La etapa de envío E175 puede realizarse de conformidad con un protocolo que comprende una etapa de cifrado y/o

una etapa de firma. En un ejemplo, el protocolo es el "Protocolo de canal seguro 80", el "Protocolo de canal seguro 81", el "Protocolo de canal seguro 02" o el "Protocolo de canal seguro 03". Estos protocolos están definidos por la norma "Plataforma Global 2.2".

Además, tal como se da a conocer con más detalle a continuación, el módulo de configuración 132 puede, en un ejemplo, tener en cuenta el elemento de información 128, 129 para elegir los métodos para enviar los datos de configuración DC más apropiados. Estos métodos son, por ejemplo, el instante de enviar los datos de configuración de CC y/o la red utilizada para este envío.

En un ejemplo, los datos de configuración de DC son datos de personalización e incluyen un script para instalar un perfil de personalización. Después de obtener los datos de configuración de DC mediante el elemento seguro 100, el elemento seguro ejecuta el script para instalar el perfil de personalización en el elemento seguro. Según la norma "ETSI TS 103.383", un perfil de personalización es una combinación de estructuras de ficheros para aplicaciones o servicios y datos de identificación y autenticación. Una vez instalado en el elemento seguro 100, una aplicación comercial utiliza este perfil de personalización para comunicarse con entidades externas al terminal 120.

En un ejemplo, el elemento de información 128, 129 es el número "IMEI" o "IMEISV" del terminal 120. El módulo de configuración 162 recupera los datos de configuración de CC (E265) que permiten instalar un perfil correspondiente al tipo de terminal 120, a partir del número "IMEI" o "IMEISV" del terminal 120.

Si el terminal 120 es un vehículo de motor, el módulo de configuración 162 determina que el perfil de personalización a instalar es un perfil de personalización que permite el envío de datos por un canal de comunicación de alta velocidad. Este canal de comunicación de banda ancha es, por ejemplo, el "GPRS" (Servicio General de Radio en Paquetes) ("General Packet Radio Service" en terminología inglesa), "UMTS" (Sistema Universal de Telecomunicaciones Móviles) ("Universal Mobile Telecommunications System" en terminología inglesa) o "HSDPA" (Acceso a Paquetes de Enlace Descendente de Alta Velocidad) ("High Speed Downlink Packet Access" en terminología inglesa). Gracias a este perfil de personalización y a la aplicación empresarial, el vehículo de motor puede ofrecer acceso a Internet o un servicio de avería a distancia.

Si el terminal 120 es una farola o un medidor eléctrico, el módulo de configuración 162 determina, preferiblemente a partir del elemento de información 128, 129, que el perfil de personalización a instalar es un perfil de personalización que utiliza un espacio de memoria reducido y que permite únicamente el envío del mensaje "SMS" (Servicio de Mensajes Cortos) ("Short Message Service" en terminología inglesa) por el terminal 120. Gracias a este perfil de personalización y a la aplicación comercial, el medidor eléctrico puede realizar una recogida de datos de consumo mediante un mensaje "SMS", o la farola se puede encender o apagar de forma distante enviando mensajes "SMS".

En otro ejemplo, el elemento de información 128, 129 es el código "MCC" (o equivalente) del terminal 120. Ello permite que el módulo de configuración 162 determine un perfil de personalización adaptado al país en donde se encuentra el terminal 120. De hecho, un operador telefónico utiliza un perfil de personalización diferente para cada país, incluyendo cada perfil de personalización algoritmos de autenticación, filtros de datos o diferentes aplicaciones para cada país. Así, el paso del terminal 120 de un país a otro se realiza sin dificultad.

En otro ejemplo, el elemento de información 128, 129 es el código "MNC" del terminal 120, lo que permite que el módulo de configuración 162 conozca la red utilizada por el terminal 120 y envíe los datos de configuración de CC a través de esta red. Además, si el elemento de información 128, 129 es el código "NMR", el módulo de configuración 162 envía los datos de configuración DC solamente cuando la cobertura de la red es de buena calidad.

Por otro lado, si el elemento de información 128, 129 indica los diferentes tipos de canales de comunicación soportados por el terminal 120 (por ejemplo, para el protocolo "BIP"), el módulo de configuración 162 puede elegir el canal de comunicación más adecuado para enviar los datos de configuración de CC en la etapa E275. Por lo tanto, el módulo de configuración puede tener en cuenta el elemento de información 128, 129 para enviar los datos de configuración DC al elemento seguro 100.

En un ejemplo particular, el terminal 120 soporta un primer canal de comunicación de alta velocidad (por ejemplo, alta velocidad) y un segundo canal de comunicación de velocidad moderada (por ejemplo, baja velocidad), el primer canal ofrece una velocidad mayor que la velocidad del segundo canal. En este caso, el módulo de configuración 162 (y más en general el sistema de configuración 160) envía los datos de configuración DC a la aplicación 108 durante la etapa E275 a través del primer canal de comunicación, es decir el canal de comunicación con la velocidad superior. En un caso particular, el módulo de configuración 162 determina a partir de los datos incluidos en el elemento de información 128, 129 que el terminal 120 soporta al menos dos canales de comunicación que ofrecen diferentes velocidades de bits y, en consecuencia, selecciona el canal de comunicación de mayor velocidad para transmitir los datos de configuración de CC a la aplicación 108 en la etapa E275.

En una forma de realización particular, el módulo de configuración 162 determina, a partir del elemento de información 128, 129, el canal de comunicación de mayor velocidad soportado por el elemento seguro 100 (o por el terminal 120), y utiliza el canal de comunicación de mayor velocidad así determinado para enviar (E275) los datos de configuración

de CC a la aplicación 102 (y más en general al elemento seguro 100).

En un ejemplo particular, cuando el terminal 120 soporta un canal de comunicación de alta velocidad, el sistema de configuración 162 transmite un primer perfil (o fichero) de personalización denominado "de gran magnitud" en la etapa E275 a la aplicación 108. Por el contrario, cuando el terminal 120 soporta un canal de comunicación con velocidad moderada, el sistema de configuración 162 transmite a la aplicación un segundo perfil (o fichero) de personalización de menor magnitud en la etapa E275 a la aplicación 108. El canal de comunicación de alta velocidad es, por ejemplo, un canal que funciona según el protocolo https. El canal de comunicación de velocidad moderada es, por ejemplo, un canal de comunicación que funciona según el protocolo SMS.

Según una puesta en práctica particular, el módulo de configuración 162 puede enviar (E275) como datos de configuración de CC a la aplicación 102 un primer perfil de personalización (o más en general un primer dato) denominado "de gran magnitud", o bien, un segundo perfil de personalización (o más en general un segundo dato) denominado "de pequeña magnitud", siendo la magnitud del primer perfil superior a la del segundo perfil. Por ejemplo, el primer perfil de gran magnitud es al menos 2, 5, 10 e incluso 20 veces más superior en términos de magnitud de datos (es decir, en número de bytes) que el segundo perfil de magnitud pequeña. En un ejemplo particular, el primer perfil de gran magnitud tiene una magnitud de 256 Kbits mientras que el segundo perfil de magnitud pequeña tiene una magnitud de 8 Kbits.

Según un ejemplo particular, el módulo de configuración 162 selecciona entre el primer y el segundo perfil que deben enviarse (E275) a la aplicación 102 (o más en general al elemento seguro 100) en función de la velocidad del canal de comunicación soportada por el terminal 120 y/o del tipo de canal de comunicación soportado por el terminal 120, siendo la velocidad del canal y/o el tipo de canal determinado preferiblemente por el módulo de configuración 162 a partir del elemento de información 128, 129.

En un ejemplo particular, el sistema de configuración 162 verifica si un canal de comunicación cuya velocidad es al menos igual a un valor umbral predeterminado puede establecerse con el elemento seguro 100 (o más en general con el terminal 120) o compruebe si se puede establecer un canal de comunicación de un tipo predeterminado con el elemento seguro (o más en general con el terminal). Esta etapa de verificación se lleva a cabo preferiblemente a partir del elemento de información 128, 129. En el caso en que dicha etapa de verificación sea positiva, el módulo de configuración 162 envía el primer perfil (de gran magnitud) en tanto como datos de configuración durante la etapa de envío (E275) al elemento seguro 100. De lo contrario, el módulo de configuración 162 envía (E275) el segundo perfil (de magnitud pequeña) en tanto como datos de configuración al elemento seguro 100.

Por ejemplo, el primer perfil de gran magnitud es particularmente adecuado para ser transmitido por un canal de comunicación de conformidad con el protocolo https. Además, el segundo perfil de pequeña magnitud es, por ejemplo, particularmente adecuado para ser transmitido por un canal de comunicación de conformidad con el protocolo SMS.

Tal como se indicó con anterioridad, el módulo de configuración 162 puede tener en cuenta el elemento de información 128, 129 para enviar los datos de configuración DC al elemento seguro 100 y, más en particular, a la aplicación 108. En un ejemplo particular, el elemento de información 128, 129 proporciona información sobre el tipo de terminal 120 (por ejemplo, si se trata de un teléfono móvil o un medidor eléctrico). El módulo de configuración 120 puede así, desde el elemento de información 128, 129 determinar al menos uno de los siguientes parámetros:

(a) los datos de configuración de CC que se enviarán (E275) a la aplicación 108 (por ejemplo, eligiendo un primer perfil de personalización denominado "de gran magnitud" o bien, un segundo perfil de personalización de menor magnitud);

(b) el canal de comunicación (o el tipo de canal), el protocolo de comunicación y/o la portadora que se utilizará para enviar (E275) los datos de configuración de CC a la aplicación 108 (para elegir, por ejemplo, el canal y/o el protocolo más adecuado para las capacidades del terminal 120).

En un ejemplo particular, el módulo de configuración 120 determina, a partir del elemento de información 128, 129 si el terminal 120 es un teléfono móvil (o más en general un terminal móvil de telecomunicaciones) o un medidor eléctrico. El módulo de configuración 120 a continuación adapta al menos uno de los parámetros (a) y (b) mencionados con anterioridad al enviar (E275) los datos de configuración de CC a la aplicación 108.

La adaptación de los parámetros (a) y/o (b) anteriores permite optimizar el envío (E275) de los datos de configuración de CC en función, en particular, de las capacidades del terminal 120 que ejecuta la aplicación 108. Por lo tanto, un medidor eléctrico es un dispositivo cuya función principal es medir la cantidad de electricidad consumida en un lugar (un hogar, una industria...). Los denominados medidores eléctricos inteligentes son, por ejemplo, capaces de llevar a cabo una recogida remota de datos de consumo por mensaje "SMS" y también de recibir los datos de configuración de CC a través del protocolo SMS. Por el contrario, dichos medidores eléctricos no son capaces, por ejemplo, de recibir a través del protocolo https los datos de configuración de CC, a diferencia de los teléfonos móviles que tienen la capacidad de comunicarse a través de Internet.

El perfil de configuración del PC también se puede utilizar para permitir que el terminal 120 se comunique con un servidor de correo electrónico, para sincronizarse con la mensajería local.

Un experto en esta técnica entenderá que las formas de realización y variantes descritas con anterioridad solamente constituyen ejemplos no limitativos de puestas en práctica de la invención. En particular, un experto en esta técnica puede prever cualquier combinación de las variantes y formas de realización descritas con anterioridad para satisfacer una necesidad muy específica.

REIVINDICACIONES

1. Método de notificación para configurar un elemento seguro (100) incorporado en un terminal (120) conectado a una red (140), comprendiendo dicho método las siguientes etapas puestas en práctica por una aplicación (108) de dicho elemento seguro:

obtener (A215) al menos un elemento de información (128, 129) útil para configurar el elemento seguro (100) almacenado en una memoria del terminal (120) externo al elemento seguro (100),

enviar (A220) dicho elemento de información (128, 129) y un identificador (ID) del elemento seguro (100) a un sistema de configuración (160), y

obtener (A275) datos de configuración (DC) procedentes del sistema de configuración (160), siendo dichos datos de configuración (DC) suministrados al elemento seguro (100) en función de dicho elemento de información (128, 129), con dichos datos de configuración (DC) siendo datos de personalización y comprendiendo un script para instalar un perfil de personalización,

en donde el elemento de información (128, 129) es uno entre el tipo de canal de comunicación soportado por el terminal y el tipo de portadora utilizado por el terminal, y se utiliza para determinar, por el sistema de configuración (160), al menos uno de elementos entre:

el canal de comunicación utilizado para enviar datos de configuración cuando el elemento de información es el tipo de canal de comunicación admitido por el terminal,

la portadora utilizada para enviar datos de configuración cuando el elemento de información es el tipo de portadora utilizado por el terminal.

2. Método de notificación según la reivindicación 1, caracterizado porque el envío de dicho elemento de información (128, 129) y del identificador (ID) del elemento seguro (100) se lleva a cabo en función con la instrucción de control Sim Tool Kit "ENVIAR SMS" o "ABRIR CANAL", definida por la norma 3GPP 31.111.

3. Método de notificación según la reivindicación 1 o 2, caracterizado porque la obtención (A215) de dicho elemento de información (128, 129) se realiza a petición de la aplicación (108) del elemento seguro (100), estando dicha demanda conforme con la instrucción de control Sim Tool Kit "PROPORCIONAR INFORMACIÓN LOCAL" definida por la norma "3GPP 31.111".

4. Elemento seguro (100) destinado a ser incorporado en un terminal (120) conectado a una red (140), comprendiendo dicho elemento seguro una aplicación (108) que comprende:

- medios para obtener al menos un elemento de información (128, 129) útil para la configuración del elemento seguro (100) almacenado en una memoria del terminal (120) externa al elemento seguro,

- medios para enviar dicho elemento de información (128, 129) y un identificador (ID) del elemento seguro a un sistema de configuración (160), y

- medios para obtener datos de configuración (DC) procedentes del sistema de configuración (160), siendo dichos datos de configuración (DC) suministrados al elemento seguro en función con dicho elemento de información (128, 129), siendo dichos datos de configuración (DC) datos de personalización y que incluyen un script de instalación de un perfil de personalización,

en donde el elemento de información (128, 129) es uno entre el tipo de canal de configuración soportado por el terminal y el tipo de portadora utilizada por el terminal, y se utiliza para determinar, por el sistema de configuración (160), al menos uno de los elementos entre:

- el canal de comunicación utilizado para enviar datos de configuración cuando el elemento de información es el tipo de canal de comunicación admitido por el terminal,

- la portadora utilizada para enviar datos de configuración cuando el elemento de información es el tipo de portadora utilizado por el terminal.

5. Terminal (120) que comprende un elemento seguro (100) según la reivindicación 4.

6. Programa informático que comprende instrucciones para la ejecución de las etapas de un método de notificación según cualquiera de las reivindicaciones 1 a 3 cuando dicho programa se ejecuta por un elemento seguro (100) incorporado en un terminal (120).

7. Medio de registro legible por un elemento seguro (100) incorporado en un terminal (120), en donde se registra un programa informático que comprende instrucciones para la ejecución de las etapas de un método de notificación según una cualquiera de las reivindicaciones 1 a 3.

8. Método para configurar un elemento seguro (100) incorporado en un terminal (120) conectado a una red (140), siendo dicho método puesto en práctica por un sistema de configuración (160), comprendiendo dicho método:

- la obtención (D220) y la memorización (D230) de al menos un elemento de información (128, 129) útil para configurar el elemento seguro (100) y un identificador (ID) del elemento seguro (100) procedente del elemento seguro (100),

- el establecimiento (D225) de un canal de comunicación seguro (CN) con el elemento seguro (100), y

- el envío (E275) de datos de configuración (DC) al elemento seguro (100) a través de dicho canal de comunicación (CN), siendo dichos datos de configuración (DC) suministrados al elemento seguro en función de dicho elemento de información (128, 129), siendo dichos datos de configuración (DC) datos de personalización y que comprenden un script para instalar un perfil de personalización,

en donde el elemento de información (128, 129) es uno entre el tipo de canal de comunicación soportado por el terminal, y el tipo de portadora usado por el terminal, y se utiliza para determinar, por el sistema de configuración (160), al menos uno de los elementos entre:

- el canal de comunicación utilizado para enviar datos de configuración cuando el elemento de información es el tipo de canal de comunicación admitido por el terminal,

- la portadora utilizada para enviar datos de configuración cuando el elemento de información es el tipo de portadora utilizado por el terminal.

9. Método según la reivindicación 1 u 8, caracterizado por cuanto que:

- el identificador (ID) del elemento seguro (100) es uno entre:

- el identificador "ID de eUICC" definido por la versión 1.46 de la especificación de "Arquitectura de aprovisionamiento distante para UICC incorporada" del " Sistema Global para la Mobile Communication Association",

- el identificador "ID de ICC" definido por la norma "ISO 7812", y

- el "IMSI".

10. Método según cualquiera de las reivindicaciones 8 a 9, que comprende una etapa de verificación para verificar si un canal de comunicación cuya tasa binaria es al menos igual a un valor umbral predeterminado puede establecerse con el elemento seguro (100) o para verificar si se puede establecer un canal de comunicación de un tipo predeterminado con el elemento seguro (100), y:

- en caso afirmativo, el envío de primeros datos en tanto como datos de configuración (DC) durante la etapa de envío (E275) al elemento seguro (100);

- en caso negativo, el envío de segundos datos en tanto como datos de configuración (DC) durante la etapa de envío (E275) al elemento seguro (100), teniendo los primeros datos una magnitud de datos mayor que los segundos datos.

11. Sistema de configuración (160) de un elemento seguro (100) incorporado en un terminal (120) conectado a una red (140), comprendiendo dicho sistema de configuración:

- un módulo de gestión (161) capaz de obtener al menos un elemento de información (128, 129) útil para la configuración del elemento seguro (100) y un identificador (ID) del elemento seguro (100) procedente del elemento seguro (100),

- un módulo de comunicación seguro (165) con el elemento seguro (100), siendo dicho módulo de comunicación seguro (165) capaz de establecer un canal de comunicación seguro (CN) con el elemento seguro (100),

- una primera memoria (163) capaz de memorizar dicho elemento de información (128, 129) y el identificador (ID) del elemento seguro (100), y

- un módulo de configuración (162) capaz de enviar datos de configuración (DC) al elemento seguro (100) a través

de dicho canal de comunicación (CN), siendo dichos datos de configuración (DC) suministrados al elemento seguro (100) en función del elemento de información (128, 129), siendo dichos datos de configuración (DC) datos de personalización y que comprenden un script para instalar un perfil de personalización,

en donde el elemento de información (128, 129) es uno entre el tipo de canal de comunicación soportado por el terminal y el tipo de portadora utilizado por el terminal, y se utiliza para determinar, por el sistema de configuración (160), al menos uno de los elementos entre:

- el canal de comunicación utilizado para enviar datos de configuración cuando el elemento de información es el tipo de canal de comunicación admitido por el terminal,

- la portadora utilizada para enviar datos de configuración cuando el elemento de información es el tipo de portadora utilizado por el terminal.

12. Programa informático que comprende instrucciones para la ejecución de las etapas de un método de configuración según cualquiera de las reivindicaciones 8 a 10, cuando dicho programa se ejecuta por un sistema de configuración (160).

13. Un medio de registro legible por un sistema de configuración (160), en donde se registra un programa informático que comprende instrucciones para la ejecución de las etapas de un método de configuración según una cualquiera de las reivindicaciones 8 a 10.

14. Sistema que comprende un terminal (120) que incluye un elemento seguro (100) según la reivindicación 4, siendo este terminal (120) y este elemento seguro (100) capaces de poner en práctica un método de notificación según cualquiera de las reivindicaciones 1 a 3 y un sistema de configuración (160) según la reivindicación 12, siendo este sistema de configuración (160) capaz de poner en práctica un método de configuración según una de las reivindicaciones 8 a 10.

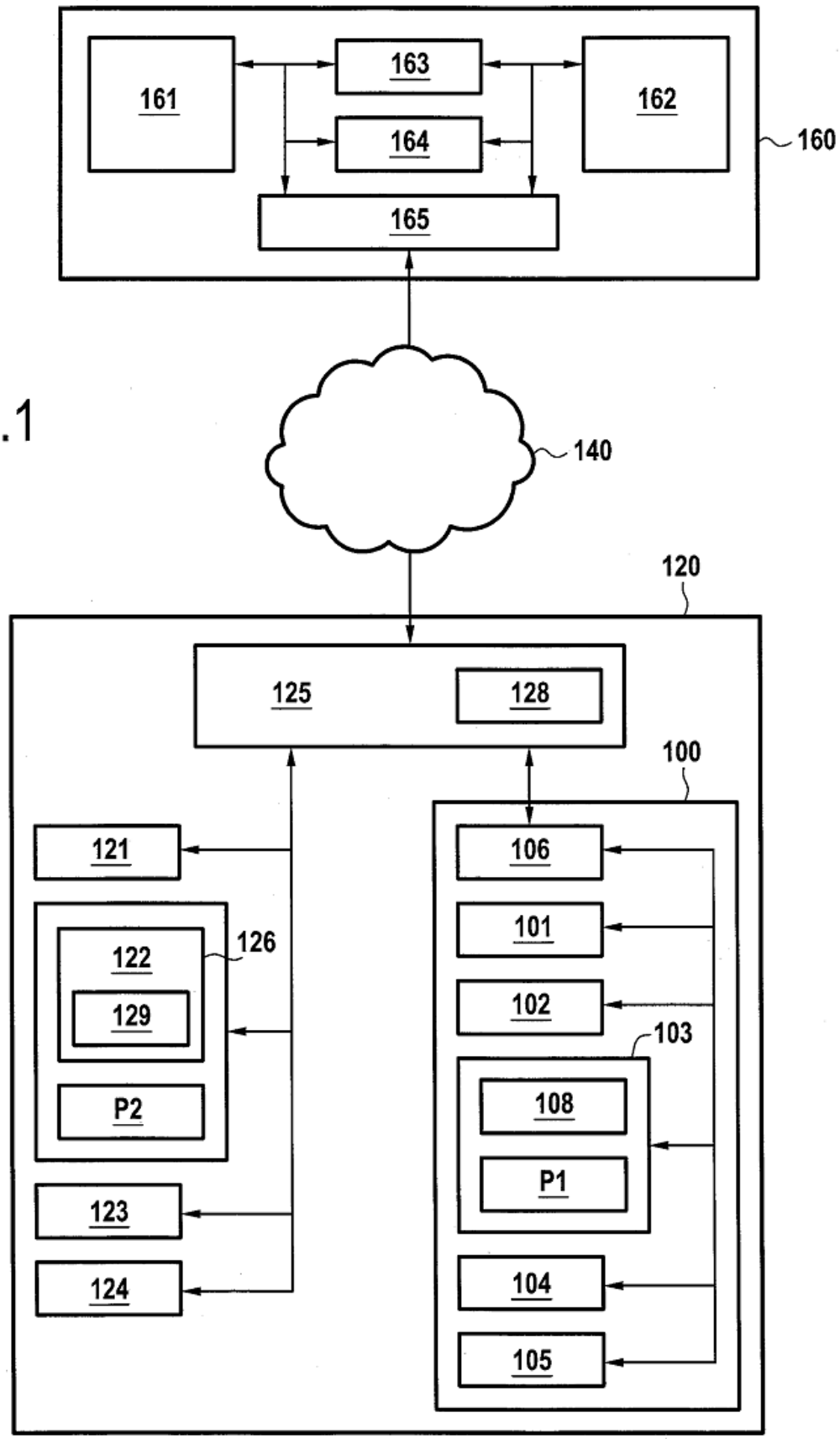
161
163
162
164
160
165
140
120
125
128
100
121
106
101
126
122
102
129
103
108
P2
P1
123
104
124
105

FIG.1

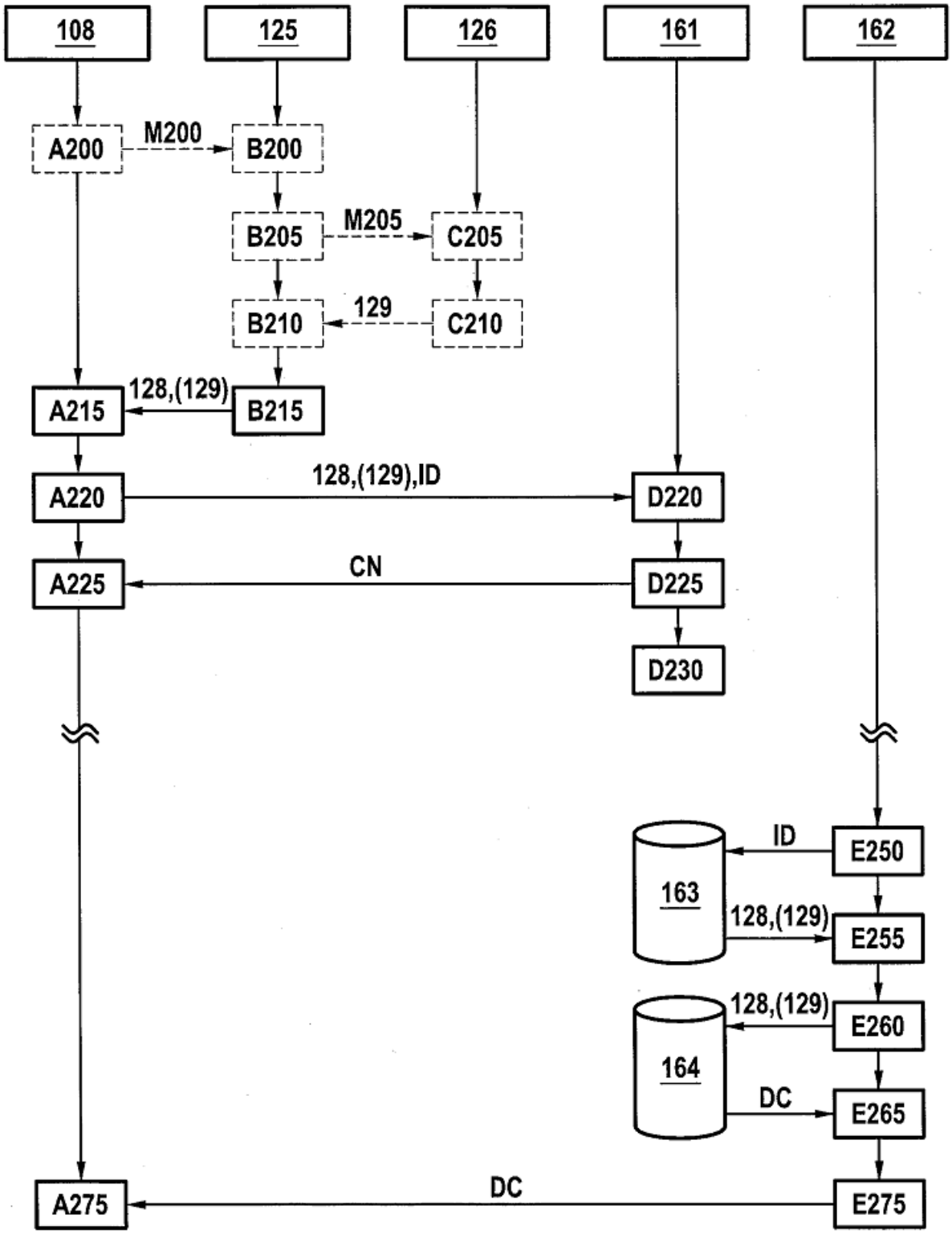
108
125
126
161
162
A200
M200
B200
B205
M205
C205
B210
129
C210
A215
128,(129)
B215
A220
128,(129),ID
D220
A225
CN
D225
D230
163
ID
E250
128,(129)
E255
164
128,(129)
E260
DC
E265
A275
DC
E275

FIG.2