(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 525 469**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/22 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.03.2009 E 09730101 (4)**

(97) Fecha y número de publicación de la concesión europea: **03.09.2014 EP 2263359**

(54) Título: **Procedimiento de acceso y de transferencia de datos relacionados con una aplicación instalada en un módulo de seguridad asociado a un terminal móvil, módulo de seguridad, servidor de gestión y sistema asociados**

(30) Prioridad:

31.03.2008 FR 0852110

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.12.2014

(73) Titular/es:

ORANGE (100.0%)
78, rue Olivier de Serres
75015 Paris , FR

(72) Inventor/es:

RAFFARD, RÉMI y
ASSADI, HOUSSEM

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Procedimiento de acceso y de transferencia de datos relacionados con una aplicación instalada en un módulo de seguridad asociado a un terminal móvil, módulo de seguridad, servidor de gestión y sistema asociados

La presente invención se refiere al campo de las telecomunicaciones y, más en particular, al de la seguridad de las aplicaciones alojadas en un elemento seguro de un terminal móvil.

La mayoría de los terminales móviles existentes permiten no sólo establecer comunicaciones telefónicas, sino también ejecutar un cierto número de aplicaciones descargadas a un módulo de seguridad relacionado con el terminal. Este módulo de seguridad puede ser un módulo de memoria del terminal o un soporte removible (por ejemplo, una tarjeta chip de abonado) insertado en el terminal.

La descarga de estas aplicaciones se realiza mediante una conexión convencional del terminal móvil con un servidor de gestión.

Tal aplicación comprende, por una parte, una parte de programa que se ejecuta en la recepción de una orden de selección de la aplicación proveniente de un equipo externo, por ejemplo una terminal sin contacto, y, por otra, un área de datos de aplicación.

Estos datos de aplicación son generados por un proveedor de servicios, por ejemplo un banco para una aplicación de pago, y transmitidos a un servidor de gestión a través de un canal seguro. A continuación de la recepción de esos datos, el servidor de gestión ordena la descarga de esos datos al módulo de seguridad, utilizando un juego de claves compartidas entre él y este módulo.

A lo largo del tiempo de vida de la aplicación, una parte de esos datos puede ser actualizada por la propia aplicación.

Para un equipo tal como un servidor de gestión, no hay medio alguno para recuperar esos datos modificados con el propósito de transferirlos hacia otro módulo de seguridad o de realizar una copia de seguridad de los mismos durante una actualización de la aplicación.

Así, en un cambio de módulo de seguridad, por ejemplo un cambio de tarjeta SIM a raíz de un cambio de operador, el usuario tiene que dirigirse al servidor de gestión que gestiona la aplicación, el cual nuevamente se dirige al proveedor de servicios de la aplicación para obtener los datos de aplicación.

Con el incremento del número de terminales móviles, son más numerosos los cambios de módulos de seguridad, y este proceso se hace difícil de gestionar.

Además, los datos de aplicación descargados son los datos iniciales y no los datos actualizados a lo largo del tiempo de vida de la aplicación. La solicitud de patente internacional WO 01/0811 A1 describe un sistema que comprende una tarjeta para el almacenamiento seguro de las aplicaciones y sus datos. La tarjeta comprende diferentes áreas de memoria para el acceso seguro.

La compañía SICAP (marca registrada) propone un producto que permite actualizar la configuración de una tarjeta SIM (por "Subscriber Identity Module"). Esta actualización consiste, para un servidor remoto, en leer los datos de configuración de una tarjeta SIM inserta en un terminal móvil y en reinscribirlos después en otra tarjeta SIM. Los datos transferidos de este modo son datos no sensibles, es decir, no confidenciales y, por consiguiente, no protegidos contra lectura. Para leer tales datos, el servidor transmite una orden de lectura de acuerdo con la norma ISO 7816-4. Este producto no permite leer información confidencial y, por tanto, no permite copiar los datos de aplicación confidenciales de una aplicación instalada en una tarjeta SIM.

Por otro lado, en una actualización de la aplicación, por ejemplo un cambio de versión del programa de la aplicación, el área de datos de aplicación se reinicializa con los datos nuevamente transmitidos por el proveedor de servicios relacionado con la aplicación.

Hay, pues, una necesidad de poder recuperar de manera segura el área de datos de aplicación y confidenciales de una aplicación, con el propósito de transferirlos hacia otro módulo de seguridad o de reinstalarla con motivo de una actualización de la aplicación, sin recurrir a un proveedor de servicios.

A tal efecto, la presente invención propone un procedimiento de gestión de datos según la reivindicación 1.

Así, los datos de aplicación de una aplicación instalada en un módulo de seguridad se pueden recuperar mediante un servidor de gestión, previa autenticación del mismo por el módulo de seguridad. A continuación, los datos recuperados por el servidor pueden ser transferidos hacia otro módulo de seguridad, sin precisar acceso al proveedor de servicios de la aplicación.

Los datos de aplicación de la aplicación también se pueden almacenar temporalmente en un área de memoria de módulo de seguridad para permitir una actualización de la aplicación. Así, se podrán reinstalar a continuación de esta actualización. Así, la actualización de una aplicación ya no precisa acceder al servidor del proveedor de servicios.

Según una característica particular del procedimiento de la invención, la petición de acceso comprende una orden de acción y el procedimiento comprende una etapa de ejecución de dicha acción tras la etapa de transmisión o de almacenamiento.

Así, la orden de acción permite precisar la petición de acceso indicando las acciones complementarias que el módulo de seguridad habrá de realizar en una petición de acceso.

Según con un modo de realización particular de la invención, la acción es un bloqueo de dicha aplicación y/o un borrado de datos de dicha aplicación. El bloqueo o el borrado de datos de la aplicación evitan que una misma instancia de la aplicación sea duplicada en varios módulos de seguridad y, así, permite aumentar la seguridad.

Según otro modo de realización, la acción es una petición de transferencia de dichos datos de la aplicación a una segunda área de memoria del módulo de seguridad. Los datos de los que se crea así copia de seguridad pueden así ser reutilizados por el módulo de seguridad, por ejemplo ser reinstalados con motivo de la actualización de la aplicación. La no comunicación de datos a un equipo exterior al módulo de seguridad permite una vez más aumentar la seguridad.

Según un modo de realización particular, el procedimiento comprende además una etapa de recepción de una orden de actualización de la aplicación en una tercera área de memoria segura y una etapa de recepción de una orden de transferencia de dichos datos de la segunda área de memoria hacia la tercera área de memoria segura.

Así, la actualización de una aplicación, por ejemplo la implantación de una nueva versión del programa de la aplicación, ya no precisa un acceso a un proveedor de servicios para la instalación de los datos de aplicación. Además, los datos de aplicación reinstalados son los datos de aplicación de los que disponía el inventor antes de la actualización y no los datos de aplicación iniciales. Así, la actualización de una aplicación se efectúa de manera transparente para el usuario y no precisa de la reconfiguración de esos datos.

De acuerdo con un modo de realización particular, el procedimiento comprende el acceso a datos relacionados con una aplicación instalada en un módulo de seguridad asociado a un terminal móvil, caracterizado por comprender:

- una etapa de transmisión de un mensaje que contiene una petición de acceso a datos seguros del módulo de seguridad, cifrándose al menos parte de dicho mensaje con una primera clave de gestión,

- una etapa de recepción de dichos datos cifrados con una segunda clave de gestión asociada a la primera clave,

- una etapa de obtención de dichos datos por descifrado por medio de la primera clave.

Así, un servidor de gestión apto para obtener esos datos puede transferirlos hacia otro módulo de seguridad sin precisar el acceso a un proveedor de servicios. Los datos obtenidos también pueden ser guardados en copia de seguridad por el servidor de gestión para, a continuación, ser retransferidos hacia el mismo módulo de seguridad, por ejemplo tras una actualización de la aplicación relacionada con los datos.

Según una característica particular, la petición de acceso comprende una orden de acción, siendo dicha acción una petición de bloqueo de la aplicación y/o una petición de borrado de datos de la aplicación.

Según otra característica particular, el procedimiento comprende además una etapa de transmisión segura de dichos datos a un segundo módulo de seguridad.

Otro modo de realización concierne asimismo a un procedimiento de petición de transferencia de datos relacionados con una aplicación instalada en un módulo de seguridad asociado a un terminal móvil, siendo almacenados los datos en una primera área de memoria segura del módulo de seguridad, caracterizado por comprender:

- una etapa de transmisión de un mensaje que contiene una petición de transferencia de dichos datos de dicha aplicación a una segunda área de memoria del módulo de seguridad, cifrándose al menos parte de dicho mensaje con una primera clave de gestión,

- una etapa de transmisión de una actualización de dicha aplicación a una tercera área de memoria segura,

- una etapa de transmisión de una petición de transferencia de dichos datos de la segunda área de memoria hacia dicha tercera área de memoria segura.

Así, la actualización no precisa acceder al servidor del proveedor de servicios y se efectúa de manera transparente para el usuario.

Otro modo de realización se refiere asimismo a un módulo de seguridad asociado a un terminal móvil, que comprende medios de recepción de un mensaje que contiene una petición de acceso a datos relacionados con una aplicación instalada en el módulo de seguridad, estando almacenados los datos en una primera área de memoria segura del módulo de seguridad, estando cifrado dicho mensaje con una primera clave de gestión, medios de obtención de dicha petición por descifrado del mensaje por medio de una segunda clave de gestión asociada a la primera clave de gestión, medios de lectura de dichos datos, medios de cifrado de los datos leídos con la segunda clave de gestión, medios de transmisión de los datos cifrados y al menos una segunda área de memoria apta para almacenar los datos cifrados.

La invención se refiere finalmente a un producto de programa de ordenador según la reivindicación 9.

Otras particularidades y ventajas de la presente invención se irán poniendo de manifiesto en la siguiente descripción de modos de realización dados a título de ejemplo no limitativo, con referencia a los dibujos que se acompañan, en los cuales:

- la figura 1 es un esquema que ilustra el contexto general de la invención,

- la figura 2 es un organigrama que ilustra las diferentes etapas de un procedimiento de acceso y de un procedimiento de transferencia de datos según la invención,

- la figura 3 es un esquema que ilustra un sistema de transferencia de datos de un primer módulo de seguridad hacia un segundo módulo de seguridad, según un modo de realización de la invención,

- la figura 4 es un esquema de bloques que ilustra un primer módulo de seguridad apto para transmitir o para almacenar datos seguros, utilizado en un sistema de transferencia según la invención,

- la figura 5 es un esquema de bloques que ilustra un segundo módulo de seguridad apto para recibir los datos seguros provenientes del primer módulo de seguridad, utilizado en un sistema de transferencia según la invención,

- la figura 6 es un organigrama que ilustra las etapas de un procedimiento de transferencia de datos y de un procedimiento de acceso a datos seguros puestas en práctica en un sistema de transferencia según un modo de realización de la invención,

- la figura 7 es un esquema que ilustra un procedimiento de petición de transferencia de datos y un procedimiento de acceso a los datos puestos en práctica en la actualización de una aplicación, según un modo de realización de la invención,

- la figura 8 es un esquema de bloques que representa un servidor de gestión apto para realizar las etapas de un procedimiento de acceso según un modo de realización de la invención,

- la figura 9 es un esquema de bloques que representa un servidor de gestión apto para realizar las etapas de un procedimiento de petición de transferencia según un modo de realización de la invención.

Se describirá a continuación, haciendo referencia a las figuras 1 y 2, un modo de realización de un procedimiento de transferencia de datos y de un procedimiento de acceso a esos datos.

Haciendo referencia a la figura 1, un usuario dispone de un terminal móvil 10, que es, por ejemplo, un teléfono móvil o un PDA (por "Personal Digital Assistant").

Este terminal móvil cuenta con un módulo de comunicación 30, por ejemplo un módulo GSM, que permite una comunicación, a través de una red de comunicación R, con servidores remotos, por ejemplo con un servidor de gestión T. Esta comunicación es, por ejemplo, una comunicación "OTA" (por "Over The Air"), es decir, una comunicación inalámbrica convencional. A título de alternativa, el terminal móvil está enlazado con la red R mediante una línea telefónica por cable.

El terminal móvil 10 incorpora asimismo un módulo de seguridad 20.

El módulo de seguridad 20 es, por ejemplo, un soporte removible de tipo SIM o UICC (por "Universal Integrated Circuit Card"), un área de memoria segura del terminal móvil o una tarjeta de memoria que aloja un elemento seguro (SD card, Embeded Secure Controler...).

El módulo 20 incorpora datos confidenciales C grabados en un área de memoria, que es una primera área de memoria segura. Estos datos confidenciales son, por ejemplo, datos protegidos contra lectura mediante una clave

compartida por el servidor de gestión T y el módulo de seguridad 20.

Convencionalmente, una clave compartida es o bien una misma clave conocida por las dos entidades, o bien un par de claves asociadas. Un ejemplo de claves asociadas es una pareja de claves de las cuales una de ellas es secreta y no la conoce más que una sola entidad y, la otra, pública, utilizada por la otra entidad.

Haciendo referencia a la figura 2, se describirán ahora las diferentes etapas de un procedimiento de transferencia de datos y de un procedimiento de acceso a esos datos según un modo de realización de la invención.

En una etapa previa (no representada), en el servidor de gestión T se ha grabado una primera clave de gestión KP1 y en el primer módulo de seguridad 20 se ha grabado una segunda clave de gestión KS1, asociada a la primera clave de gestión.

En una primera etapa E1, el servidor de gestión T transmite al módulo de seguridad un mensaje m1 que contiene una petición de acceso DA a los datos confidenciales C. El mensaje m1 es cifrado por el servidor T con la primera clave de gestión KP1.

Este mensaje es recibido por el módulo de seguridad 20 en una etapa E2.

En la siguiente etapa E3, el módulo de seguridad 20 descifra el mensaje m1 recibido utilizando la segunda clave de gestión KS1, y obtiene la petición de acceso DA.

En la siguiente etapa E4, el módulo de seguridad 20 analiza esta petición de acceso DA y determina que esta petición es una orden segura de lectura de los datos confidenciales C.

La etapa E4 viene seguida de una etapa E5, durante la cual el módulo de seguridad recupera esos datos C mediante lectura de la primera área de memoria segura del módulo de seguridad 20.

En la etapa E6 siguiente, el módulo de seguridad 20 cifra los datos leídos C con ayuda de la clave KS1 y, en una etapa E7, transmite un mensaje m2 que contiene los datos cifrados al servidor de gestión T, a través del terminal móvil 10 y la red R.

El servidor de gestión T recibe el mensaje m2 en una etapa E8 y, con ayuda de la clave KP1, descifra los datos contenidos en este mensaje y obtiene así los datos confidenciales C (etapa E9). Los datos obtenidos o bien se almacenan en una memoria del servidor T, o bien se transfieren a otro módulo de seguridad.

A título alternativo, las etapas E7 a E9 se sustituyen por una etapa en cuyo transcurso el módulo de seguridad 20 graba los datos cifrados en una segunda área de memoria del módulo de seguridad.

Se describirá ahora, haciendo referencia a las figuras 3 a 5, un modo de realización particular de un procedimiento de transferencia de datos y de un procedimiento de acceso a esos datos, en el que los datos seguros son transferidos de un primer módulo de seguridad hacia un segundo módulo de seguridad.

Haciendo referencia a la figura 3, un usuario dispone de un primer terminal móvil 100, que es, por ejemplo, un teléfono móvil o un PDA (por "Personal Digital Assistant").

Este terminal móvil cuenta con un módulo de comunicación 130, por ejemplo un módulo GSM, que permite una comunicación, a través de una red de comunicación R, con servidores remotos, por ejemplo con un primer servidor de gestión T1. Esta comunicación es, por ejemplo, una comunicación "OTA" (por "Over The Air"), es decir, una comunicación inalámbrica convencional.

El terminal móvil 100 incorpora asimismo un primer módulo de seguridad 120.

El primer servidor de gestión T1, por ejemplo un servidor de un proveedor de servicios, permite gestionar una o varias aplicaciones instaladas en el primer módulo de seguridad 120. Este servidor T1 se encarga en particular de la descarga de las aplicaciones que gestiona en el primer módulo de seguridad 120.

Ese usuario dispone asimismo de un segundo terminal móvil 200 que es, por ejemplo, un teléfono móvil o un PDA (por "Personal Digital Assistant").

Este terminal móvil 200 cuenta con un módulo de comunicación 230, por ejemplo un módulo GSM, que permite una comunicación, a través de la red de comunicación R, con servidores remotos, por ejemplo con un segundo servidor de gestión T2. Esta comunicación es, por ejemplo, una comunicación "OTA" (por "Over The Air"), es decir, una comunicación inalámbrica convencional.

El terminal móvil 200 incorpora asimismo un módulo seguro 220, que es un segundo módulo de seguridad.

El segundo servidor de gestión T2 permite gestionar una o varias aplicaciones instaladas en el segundo módulo de seguridad 220.

En este modo de realización, los módulos de seguridad 120 y 220 son tarjetas de memoria removibles, compatibles con las especificaciones de GlobalPlatform (GlobalPlatform Card Specification - versión 2.1.1 de marzo de 2006).

Haciendo referencia a la figura 4, se describirá ahora un modo de realización del módulo de seguridad 120, que es un módulo de seguridad apto para transmitir datos seguros.

El módulo de seguridad 120 comprende en particular un microprocesador 122, un módulo de emisión-recepción 124, una o varias memorias de tipo RAM 125 y una o varias memorias de tipo ROM o EEPROM 126 en las que se graban programas que pueden ser ejecutados por el microprocesador 122.

De conformidad con las especificaciones de GlobalPlatform, en el módulo de seguridad 120 se ha definido un dominio de seguridad SD1. Este dominio de seguridad es un área de memoria 126 del módulo de seguridad protegida mediante una clave K1c compartida con el servidor de gestión T1. La clave K1c es, por ejemplo, una clave, llamada clave diversificada, determinada por el servidor de gestión T1 a partir de una clave maestra K1 conocida únicamente por el servidor de gestión T1.

A título alternativo, el módulo de seguridad 120 puede contener varios dominios de seguridad, quedando protegido cada dominio mediante una clave transmitida por un servidor de gestión.

Mediante el primer servidor de gestión T1, se ha instalado en el primer módulo de seguridad 120, asociado al terminal móvil 100, una aplicación, por ejemplo una aplicación de pago AP1.

La descarga de esta aplicación comprende convencionalmente tres fases: la descarga del programa P1 de la aplicación, la instanciación y la personalización.

La descarga del programa P1 de la aplicación AP1 se efectúa bien sea en un área ZP1 del dominio de seguridad SD1, o bien en un área de memoria, del módulo de seguridad, común para todos los dominios de seguridad del módulo de seguridad 120.

La instanciación de la aplicación AP1 en el dominio de seguridad SD1 consiste en reservar un área de memoria ZD1 para la aplicación AP1 en el dominio de seguridad SD1 y en inscribir datos en esa área reservada. Más exactamente, el área ZD1 contiene un área ZDP1 de datos asociados al programa P1 y un área ZDA1 de datos de aplicación DAP1 de la aplicación AP1. Los datos asociados al programa P1 se inscriben durante la instanciación en el área ZDP1.

El área ZDA1 de datos de aplicación contiene datos actualizados a lo largo del tiempo de vida de la aplicación. Estos datos representan, por ejemplo, las elecciones de configuración de la aplicación efectuadas por el usuario o la lista de las transacciones realizadas. El área ZDA1 de datos de aplicación puede contener asimismo claves de aplicación, es decir, claves necesarias para el funcionamiento de la aplicación. Los datos de aplicación son inicializados en el módulo de seguridad, en la fase de personalización.

El área ZD1 no es accesible por lectura mediante la utilización de una orden convencional de lectura de datos, ya que es confidencial. Sólo el programa P1 de la aplicación AP1 tiene acceso, para sus propias necesidades, a esta área.

Ahora, el usuario desea que esta aplicación AP1 sea transferida al segundo módulo de seguridad 220. En concreto, este desea que el área ZDA1 de datos de aplicación de la aplicación AP1 sea transferida para así volver a tener sus elecciones de configuración en la utilización de la aplicación AP1 a partir de un terminal asociado al segundo módulo de seguridad 220.

Se describirá ahora, haciendo referencia a la figura 5, un modo de realización de un segundo módulo de seguridad 220, que es un módulo de seguridad apto para recibir los datos seguros provenientes de un primer módulo de seguridad.

El módulo de seguridad 220 comprende en particular un microprocesador 222, un módulo de emisión-recepción 224, una o varias memorias de tipo RAM 225 y una o varias memorias de tipo ROM o EEPROM 226 en las que se graban programas que pueden ser ejecutados por el microprocesador 222.

El segundo módulo de seguridad 220 contiene un dominio de seguridad SD2, conforme con las especificaciones Global Platform. Este dominio de seguridad es un área de memoria 226 del módulo de seguridad 220. Este dominio de seguridad SD2 contiene una clave de cifrado K2c compartida con el segundo servidor de gestión T2. La clave K2c es, por ejemplo, una clave determinada por el servidor de gestión T2 a partir de una clave maestra K2 conocida

únicamente por el servidor de gestión T2.

En una etapa previa, se ha descargado en el módulo de seguridad SD2 la aplicación AP1. Más exactamente, el programa P1 de la aplicación AP1 se ha descargado en un área ZP2 del módulo de seguridad SD2, y se ha reservado un área de datos ZD2 en el dominio de seguridad SD2. Además, en un área ZDP2 del área ZD2, se ha descargado el área ZDP1 de datos relacionados con la aplicación AP1.

Haciendo referencia a la figura 6, se describirán ahora las diferentes etapas de un modo de realización de un procedimiento de transferencia de datos y de un procedimiento de acceso a esos datos.

En una primera etapa E10, el primer servidor de gestión T1 establece un canal de comunicación seguro con el dominio de seguridad SD1. El establecimiento de tal canal consiste, para el primer servidor de gestión T1, en seleccionar el dominio de seguridad utilizando un identificador de ese dominio de seguridad.

Como consecuencia del establecimiento de ese canal, el servidor de gestión T1 transmite al primer módulo de seguridad 120, en una etapa E11, un mensaje m10 que contiene una petición de acceso DA a los datos de aplicación DAP1 de la aplicación AP1, almacenados en el dominio de seguridad SD1. Más exactamente, la petición de acceso DA es un nuevo mandato cuyo formato es conforme con las especificaciones GlobalPlatform. Este mandato define, en uno o varios bytes, la acción que ha de realizar el módulo de seguridad 120.

En el modo de realización descrito, la petición de acceso DA tiene la forma de un mandato normalizado APDU (por "Application Protocol Data Unit") convencional: CLA-INS-P1-P2-Lc-Data-Le. El significado general de cada parámetro CLA, INS, P1, P2, Le, Data y Le queda definido en las especificaciones ISO 7816-4.

Más exactamente, para este nuevo mandato DA, el parámetro INS es, por ejemplo, un valor que indica que la orden que ha de realizar el módulo de seguridad es una orden de lectura segura, los parámetros P1 y P2 son, por ejemplo, parámetros que especifican opciones de la orden INS, por ejemplo lectura con o sin bloqueo de la aplicación, lectura con o sin borrado de los datos... y el parámetro Data contiene, por ejemplo, un identificador de la aplicación AP1.

El mensaje m10 contiene un identificador del dominio de seguridad SD1 y la petición de acceso DA cifrada por el primer servidor T1 con la primera clave de cifrado K1c.

Como alternativa, sólo se cifra parte de la petición de acceso DA.

Este mensaje m10 es recibido por el primer módulo de seguridad 120 en una etapa E12.

En la siguiente etapa E13, el primer módulo de seguridad descifra el mensaje m10 utilizando la clave de cifrado K1c y obtiene la petición de acceso DA.

El descifrado permite al módulo de seguridad autenticar al servidor emisor de la petición.

En la siguiente etapa E14, el módulo de seguridad 120 analiza esta petición de acceso y determina que esta petición es una orden segura de lectura, mediante lectura del valor del parámetro INS. Asimismo, determina que el área solicitada es el área de datos de aplicación de la aplicación AP1 en el dominio SD1 mediante lectura del área Data contenida en el mandato DA.

La etapa E14 viene seguida de una etapa E15, en la cual el primer módulo de seguridad 120 recupera esos datos mediante lectura del área ZDA1 de datos de aplicación DAP1 de la aplicación AP1 almacenada en el dominio de seguridad SD1. El área ZDA1 representa una primera área de memoria segura.

En la etapa E16 siguiente, el primer módulo de seguridad 120 cifra los datos leídos en la etapa E15, con la clave K1c y transmite, en una etapa E17, un mensaje m20 que contiene los datos cifrados obtenidos, al primer servidor de gestión T1, a través del primer terminal móvil 100 y la red de comunicación R.

El servidor de gestión T1 recibe el mensaje m20 en una etapa E18 y, con ayuda de la clave K1c, descifra ese contenido y obtiene así el contenido DAP1 del área de datos de aplicación ZDA1 de la aplicación AP1 almacenada en el dominio de seguridad SD1 (etapa E19).

La etapa E19 viene seguida de una etapa E20 en la cual el módulo de seguridad ordena el bloqueo de la aplicación AP1. Para ello, modifica un registro Global Platform del módulo de seguridad (paso al estado "locked"). Así, la aplicación AP1 deja de responder a las peticiones de selección provenientes de equipos exteriores.

La modificación de ese registro corresponde a la ejecución de un mandato convencional Set Status, definido en las especificaciones Global Platform, transmitido por un servidor de gestión.

A título alternativo, la etapa E20 no es una etapa de bloqueo de la aplicación, sino una etapa de borrado de los datos

de la aplicación. Por ejemplo, se ponen a valor 0 todos los datos del área ZD1 y/o del área ZP1, impidiendo así cualquier ejecución de la aplicación AP1.

Aún a título alternativo, en la etapa E20 no se realiza ninguna acción.

En el modo de realización aquí descrito, la acción que ha de realizarse en la etapa E20 viene determinada por el contenido de los parámetros P1 y/o P2 de la petición de acceso DA.

Por ejemplo, el parámetro P1 es un byte con la forma 'b8 b7 b6 b5 b4 b3 b2 b1' en el que el bit B5 = 1 indica que la acción que ha de realizarse es un borrado de los datos y el bit b6 = 1 indica que el módulo de seguridad tiene que ordenar el bloqueo de la aplicación.

En una variante del modo de realización, como consecuencia de la transferencia de los datos hacia el primer servidor de gestión T1 (etapa E17), el módulo de seguridad 120 transmite una información a un servidor SP, que es, por ejemplo, un servidor del operador o del emisor del módulo de seguridad, para informarle de la transferencia de datos de aplicación, con el fin de que este guarde un historial de las transferencias realizadas para asegurar un servicio en caso de conflicto y aumentar así la seguridad del sistema.

La etapa E20 viene seguida de una etapa E21, en la cual el primer servidor de gestión T1 establece entonces un canal seguro con el segundo servidor de gestión T2. Este canal se puede establecer convencionalmente mediante el intercambio de claves compartidas entre los dos servidores.

Como consecuencia del establecimiento de ese canal seguro, el primer servidor T1 transmite al segundo servidor de gestión T2 un mensaje m30 cifrado que contiene los datos de aplicación DAP1 de la aplicación AP1, en una etapa E22.

En la etapa E23 siguiente, el segundo servidor de gestión T2 recibe estos datos y prepara un mandato de personalización de la aplicación AP1 en el dominio de seguridad SD2.

En el modo de realización aquí descrito, esta petición está constituida por una orden "Install for perso" y por una o varias órdenes "Store Data" que contienen los datos de aplicación DAP1 de la aplicación AP1 transmitidos por el servidor T1. Las órdenes "Install for perso" y "Store Data" están definidas en las especificaciones Global Platform.

A título alternativo, también los datos de aplicación son cifrados con la clave Kc2.

Estas órdenes se transmiten a continuación, cifradas con la clave de gestión Kc2 del dominio de seguridad SD2, en varios mensajes m40 al segundo módulo de seguridad 220, en una etapa E24.

En la etapa E25 siguiente, el segundo módulo de seguridad 220, tras recibir estas órdenes, las descifra y ordena la escritura de los datos de aplicación DAP1 de la aplicación AP1 en el área reservada ZD2 para la aplicación AP1 en el dominio de seguridad SD2 del segundo módulo de seguridad. Más exactamente, estos datos son grabados en el área de datos de aplicación ZDA2 de la aplicación AP1 del dominio de seguridad SD2.

En la etapa E26 siguiente, el segundo módulo de seguridad 220 devuelve un mensaje de confirmación m50 al segundo servidor de gestión T2. En el modo de realización descrito, este mensaje es una orden de confirmación (Proof of Receipt) conforme con la norma Global Platform.

El segundo servidor de gestión T2 transmite este mensaje de notificación m50 al primer servidor T1, en una etapa E27.

En un modo de realización en el que no se ha efectuado ninguna acción en la etapa E20, el primer servidor T1 puede ordenar entonces, en una etapa E28, una acción de bloqueo y/o de borrado de datos, al primer módulo de seguridad 120, como consecuencia de la recepción del mensaje m50. Para ello, transmite al módulo de seguridad 120 un mandato convencional de bloqueo (mandato Set Status especificado en Global Platform) de la aplicación AP1 y/o un mandato convencional de borrado (mandato Delete especificado en Global Platform) de los datos de aplicación relacionados con la aplicación contenidos en el dominio de seguridad SD1 del módulo de seguridad 120 y/o una orden de borrado del área de datos ZD1 y del área de programa ZP1 de la aplicación AP1.

Así, el usuario del primer módulo de seguridad ya no puede utilizar la aplicación AP1 a partir de este primer módulo de seguridad.

El primer servidor T1 también puede enviar un mensaje de información al proveedor de servicios, por ejemplo el banco, para informarle de que la aplicación AP1 ya no está accesible en el primer módulo de seguridad 120.

En el modo de realización descrito, la descarga de la aplicación AP1 en el dominio de seguridad SD2 del módulo de seguridad 220 se realiza antes de la recuperación de los datos en el primer módulo de seguridad 120. A título de

alternativa, esta descarga se puede efectuar justo antes de la transmisión de los datos de aplicación al módulo de seguridad 220, es decir, tras la etapa E21.

En el modo de realización descrito, los datos de aplicación de una aplicación son transferidos de un primer servidor de gestión T1 hacia un segundo servidor de gestión T2. La invención se aplica igualmente al caso en el que un mismo servidor de gestión gestiona los dos módulos de seguridad 120 y 220. En tal caso, no se realizan la etapa de establecimiento de canal seguro E21 y la etapa de transferencia E22 de un primer servidor al segundo servidor.

La invención se aplica igualmente al caso en el que el usuario dispone de un sólo terminal móvil y de dos módulos de seguridad. El usuario debe insertar entonces el primer módulo de seguridad en el terminal para la fase de lectura de los datos. A continuación, debe sustituir ese primer módulo, en el terminal móvil, por el segundo módulo. Finalmente, si en la fase de lectura no se ha realizado la etapa de bloqueo de la aplicación, debe reinsertar nuevamente el primer módulo.

Se describirá ahora un modo de realización de un procedimiento de petición de transferencia de datos y del procedimiento de acceso a esos datos.

Haciendo referencia a la figura 7, un usuario dispone de un terminal móvil 300 asociado a un módulo de seguridad 320.

El terminal móvil 300 cuenta asimismo con un módulo de comunicación 330 que permite una comunicación, a través de una red de comunicación R, con servidores remotos, por ejemplo con un servidor de gestión T3.

El módulo de seguridad 320 es una tarjeta de memoria compatible con las especificaciones Global Platform. Este módulo de seguridad es similar al módulo de seguridad 120, descrito anteriormente con referencia a la figura 4.

En este módulo de seguridad se ha definido un dominio de seguridad SD3. Mediante el servidor de gestión T3, para este dominio de seguridad SD3 se ha definido y grabado, en el módulo de seguridad 320, una clave de cifrado Kc3.

En este módulo de seguridad se ha instalado una aplicación AP2. Más exactamente, se graba el programa P3 de la aplicación AP2 en un área ZP3 del dominio de seguridad SD3 y se reserva para esta aplicación un área ZD3 del dominio de seguridad SD3. Los datos de aplicación DAP3 relacionados con la aplicación AP2 se han grabado en un área ZDA3 del área ZD3. El área ZDA3 representa una primera área de memoria segura.

El proveedor de servicios asociado a la aplicación AP2 desea efectuar una actualización de la aplicación AP2 y transmite al servidor de gestión T3 un nuevo programa P4 de la aplicación AP2.

El servidor de gestión T3 transmite entonces al módulo de seguridad 320 una petición de acceso a los datos de aplicación de la aplicación AP2 almacenados en el dominio de seguridad SD3. Esta petición de acceso es cifrada con la clave Kc3.

Esta petición de acceso contiene una información, que representa una orden de acción, que indica al módulo de seguridad que los datos de aplicación deben ser almacenados temporalmente, por el módulo de seguridad, en una segunda área de memoria del módulo de seguridad.

En el modo de realización aquí descrito, la petición de transferencia es un nuevo mandato cuyo formato es conforme con las especificaciones GlobalPlatform. Este mandato define, en uno o varios bytes, la acción que ha de realizar el módulo de seguridad 320.

La petición de transferencia tiene la forma: CLA-INS-P1-P2-Lc-Data-Le, con:

- INS, un parámetro que indica que la orden que ha de realizar el módulo de seguridad es una orden de transferencia,

- P1 y P2 son parámetros que especifican opciones de la orden INS, por ejemplo P1 y/o P2 indica que los datos tienen que ser transferidos de una aplicación hacia una memoria temporal,

- Data contiene un identificador de la aplicación AP2.

El módulo de seguridad recibe este mensaje y lo descifra. A continuación, accede a los datos de aplicación solicitados mediante la lectura del área ZDA3, cifra los datos leídos con la clave Kc3 y almacena los datos leídos y cifrados en una memoria temporal MT del módulo de seguridad. El área MT es una segunda área de memoria del módulo de seguridad 320.

El módulo de seguridad 320 transmite a continuación un mensaje de confirmación al servidor de gestión T3.

El servidor de gestión T3 ordena a continuación la instalación de la nueva versión de la aplicación en el dominio de seguridad SD3 del módulo de seguridad 320. Esta instalación consiste en cargar la nueva versión P4 del programa de la aplicación, en instanciarla y en activarla.

En el modo de realización descrito, estas acciones corresponden a los mandatos "Install For Load", "Load", "Install for Install" e "Install for Make Selectable" especificadas en Global Platform.

La transmisión de este nuevo programa trae consigo, de manera conocida, el borrado de las áreas ZP3 y ZD3 en el dominio de seguridad SD3 y la creación de nuevas áreas ZP4 y ZD4 en el dominio de seguridad SD3, equivalentes a las áreas ZP3 y ZD3.

En un modo de realización particular, las áreas ZP3 y ZP4, por una parte, y las áreas ZD3 y ZD4, por otra, son las mismas áreas. En tal caso, la primera área de memoria segura y la tercera área de memoria segura son las mismas.

El nuevo programa P4 se graba en el área ZP4.

Como consecuencia de la instalación de esta nueva versión P4, el módulo de seguridad envía un mensaje de confirmación al servidor de gestión T3.

El servidor de gestión T3 transmite a continuación, al módulo de seguridad 320, un mensaje que contiene una petición de transferencia de los datos de aplicación de la segunda área de memoria hacia el área ZDA4 de datos de aplicación ZDA4 de la aplicación AP2 en el dominio de seguridad SD3. El área ZDA4 queda incluida en el área ZD4 y representa una tercera área de memoria segura.

En el modo de realización aquí descrito, la petición de transferencia es un nuevo mandato cuyo formato es conforme con las especificaciones GlobalPlatform. Este mandato define, en uno o varios bytes, la acción que ha de realizar el módulo de seguridad 320.

La petición de transferencia tiene la forma: CLA-INS-P1-P2-Lc-Data-Le, con:

- INS, un parámetro que indica que la orden que ha de realizar el módulo de seguridad es una orden de transferencia,

- P1 y P2 son parámetros que especifican opciones de la orden INS, por ejemplo P1 y/o P2 indica que los datos tienen que ser transferidos de una memoria temporal hacia una aplicación,

- Data contiene un identificador de la aplicación AP2.

A título de alternativa, la petición de transferencia de los datos de la segunda área MT hacia el área de datos de aplicación de la aplicación AP2, es decir, la tercera área de memoria segura, es una orden "Install for Perso" especificada en las especificaciones Global Platform, en la que se modifica un parámetro, por ejemplo P1 o P2, para indicar que los datos de aplicación que han de transferirse están grabados en una segunda área de memoria del módulo seguro.

Como consecuencia de la recepción de este mandato, el módulo de seguridad descifra, con la clave Kc3, los datos grabados en la segunda área de memoria MT y los inscribe en el área ZDA4 reservada para los datos de aplicación de la aplicación AP2 en el dominio de seguridad SD3 del módulo de seguridad 320.

Así, el módulo de seguridad SD3 realiza las etapas de recepción de un mensaje que contiene una petición de acceso a los datos de aplicación de la aplicación AP2, grabados en una primera área segura del módulo de seguridad, estando cifrado el mensaje con una primera clave de gestión, de obtención de la petición de acceso por descifrado del mensaje por medio de una segunda clave de gestión asociada a la primera clave de gestión, de lectura de los datos de aplicación de la aplicación AP2, de cifrado de los datos leídos y de almacenamiento de los datos leídos y cifrados en una segunda área de memoria del módulo de seguridad.

El servidor de gestión T3 realiza las etapas de transmisión de un mensaje que contiene una petición de transferencia a una segunda área de memoria del módulo de seguridad de los datos de aplicación de la aplicación AP2, grabados en una primera área segura del módulo de seguridad, cifrándose el mensaje con una primera clave de gestión, de transmisión de una actualización de la aplicación AP2 a una tercera área de memoria segura y de transmisión de una petición de transferencia de los datos grabados en la segunda área de memoria hacia la tercera área de memoria segura.

En una variante de este modo de realización, los datos leídos de la primera área de memoria segura del dominio de seguridad del terminal móvil son transmitidos al servidor de gestión, el cual los graba y los transfiere nuevamente hacia el módulo de seguridad cuando se ha actualizado la aplicación.

En otra variante de este modo de realización, la nueva versión P4 del programa se instala en nuevas áreas ZP4 y ZD4 del dominio de seguridad SD3, mientras que la versión P3 de la aplicación AP2 sigue estando activa en las áreas ZP3 y ZD3. La transferencia de los datos de aplicación del área SD3 hacia el área SD4 se realiza entonces mediante una sola petición de transferencia. Esta petición de transferencia es una orden de transferencia de una primera área de memoria segura hacia una tercera área de memoria segura. Esta contiene un identificador de la primera área de memoria y un identificador de la tercera área de memoria. En esta variante, los datos leídos del área SD3 son reinscritos directamente en el área SD4.

Según un modo de realización escogido y representado en la figura 7, un servidor de gestión que pone en práctica un procedimiento de acceso según la invención es, por ejemplo, un microordenador 500 que incorpora, de manera conocida, una unidad de procesamiento 502 equipada con un microprocesador, una memoria de sólo lectura de tipo ROM o EEPROM 503, una memoria de acceso aleatorio de tipo RAM 504 y una interfaz de comunicación 505 con una red R.

El microordenador 500 puede incorporar, de manera convencional y no exhaustiva, los siguientes elementos: un teclado, una pantalla, un micrófono, un altavoz, un lector de disco, un medio de almacenamiento...

Este servidor 500 comprende un módulo de emisión de datos ME1 hacia una red de comunicación, un módulo de recepción de datos MR1 con origen en la red de comunicación, un módulo de construcción de mensaje MC1 y un módulo de cifrado y de descifrado MD1.

Una primera clave de gestión es grabada en la memoria de sólo lectura 503.

El módulo de construcción de mensaje MC1 es apto para preparar un mensaje que contiene una petición de acceso a datos seguros de un módulo de seguridad. El módulo de cifrado / descifrado MD1 es apto para cifrar al menos parte del mensaje preparado por el módulo MC1, con la primera clave de gestión grabada en la memoria de sólo lectura 503.

El módulo de transmisión ME1 es apto para transmitir el mensaje preparado y cifrado.

El módulo de recepción MR1 es apto para recibir datos cifrados con una segunda clave de gestión asociada a la primera clave de gestión y para transmitirlos al módulo de cifrado / descifrado MD1.

El módulo de cifrado / descifrado MD1 es apto para descifrar los datos cifrados recibidos, por medio de la primera clave de gestión, y para obtener así los datos solicitados.

El módulo de cifrado / descifrado MD1 es asimismo apto para cifrar esos datos con una clave compartida con una segunda entidad, por ejemplo un segundo servidor o un segundo módulo de seguridad, y el módulo de transmisión ME1 es apto para transmitir esos datos cifrados al segundo servidor o al segundo módulo de seguridad.

La memoria de sólo lectura 503 incorpora registros que guardan en memoria un programa de ordenador PG1 que incorpora instrucciones de programa adaptadas para llevar a la práctica un procedimiento de acceso según la invención tal y como se ha descrito anteriormente.

Este programa PG1 está adaptado así para transmitir un mensaje que contiene una petición de acceso a datos seguros del módulo de seguridad, cifrándose al menos parte de dicho mensaje con una primera clave de gestión, para recibir datos cifrados con una segunda clave de gestión asociada a la primera clave y para obtener los datos solicitados mediante descifrado por medio de la primera clave.

Los datos obtenidos o bien se almacenan en una memoria temporal, o bien se transfieren de manera segura, a través de la red R, a otro módulo de seguridad.

En el encendido, el programa PG1 almacenado en la memoria de sólo lectura 503 es transferido a la memoria de acceso aleatorio, la cual contendrá entonces el código ejecutable del procedimiento de presentación visual de la invención, así como registros para guardar en memoria las variables necesarias para la puesta en práctica de la invención.

De manera más general, un medio de almacenamiento, legible por un ordenador o por un microprocesador, integrado o no en el dispositivo, eventualmente removible, guarda en memoria un programa que lleva a la práctica el procedimiento de acceso a datos según la invención.

Según un modo de realización escogido y representado en la figura 8, un servidor de gestión que pone en práctica un procedimiento de petición de transferencia según la invención es, por ejemplo, un ordenador de tipo PC 600 que incorpora, de manera conocida, una unidad de procesamiento 602 equipada con un microprocesador, una memoria de sólo lectura de tipo ROM 603, una memoria de acceso aleatorio de tipo RAM 604. El terminal 600 puede incorporar, de manera convencional y no exhaustiva, los siguientes elementos: un teclado, una pantalla, un

micrófono, un altavoz, una interfaz de comunicación, un lector de disco, un medio de almacenamiento...

Este servidor comprende un módulo de emisión de datos ME2 hacia una red de comunicación, un módulo de recepción de datos MR2 con origen en la red de comunicación, un módulo de construcción de mensaje MC2 y un módulo de cifrado y de descifrado MD2.

Una primera clave de gestión es grabada en la memoria 603.

El módulo de construcción de mensaje MC2 está adaptado para preparar un mensaje que contiene una petición de transferencia de datos relacionados con una aplicación, almacenados en una primera área de memoria segura de un módulo de seguridad, a una segunda área de memoria del módulo de seguridad.

El módulo de cifrado / descifrado MD2 es apto para cifrar al menos parte del mensaje preparado por el módulo MC2, con la primera clave de gestión grabada en la memoria de sólo lectura 603.

El módulo de transmisión ME2 es apto para transmitir el mensaje preparado y cifrado.

El módulo de transmisión ME2 es asimismo apto para transmitir una actualización de una aplicación a una tercera área de memoria segura y una petición de transferencia de datos seguros de la segunda área de memoria hacia la tercera área de memoria segura.

La memoria de sólo lectura 603 incorpora registros que guardan en memoria un programa de ordenador PG2 que incorpora instrucciones de programa adaptadas para llevar a la práctica un procedimiento de petición de transferencia según la invención tal y como se ha descrito anteriormente.

Este programa PG2 está adaptado así para transmitir un mensaje que contiene una petición de acceso a datos seguros del módulo de seguridad, cifrándose al menos parte de dicho mensaje con una primera clave de gestión, para transmitir una actualización de la aplicación a una tercera área de memoria segura y para transmitir una petición de transferencia de los datos de la segunda área de memoria hacia la tercera área de memoria segura.

En el encendido, el programa PG2 almacenado en la memoria de sólo lectura 603 es transferido a la memoria de acceso aleatorio, la cual contendrá entonces el código ejecutable de la invención, así como registros para guardar en memoria las variables necesarias para la puesta en práctica de la invención.

De manera más general, un medio de almacenamiento, legible por un ordenador o por un microprocesador, integrado o no en el dispositivo, eventualmente removible, guarda en memoria un programa que lleva a la práctica el procedimiento de petición de transferencia de datos según la invención.

REIVINDICACIONES

1. Procedimiento de gestión de datos (DAP1) relacionados con una aplicación (AP1, AP2) instalada en un módulo de seguridad (20, 120, 320) asociado a un terminal móvil (10, 100, 300), estando almacenados los datos en una primera área de memoria segura (C, ZDA1) del módulo de seguridad, caracterizado porque comprende:

- una etapa de recepción (E2, E12) de un mensaje que contiene una petición de acceso a dichos datos de dicha aplicación, cifrándose al menos parte de dicho mensaje con una primera clave de gestión (KS1, Kc1, Kc3),

- una etapa de obtención (E3, E13) de dicha petición mediante descifrado del mensaje por medio de una segunda clave de gestión (KP1, Kc1) asociada a la primera clave de gestión,

- una etapa de lectura (E5, E15) de dichos datos de la aplicación,

- una etapa de cifrado (E6, E16) de los datos leídos con la segunda clave de gestión,

- una etapa de transferencia, a una segunda área de memoria segura, de los datos cifrados.

2. Procedimiento de gestión según la reivindicación 1, caracterizado porque la segunda área de memoria está situada en dicho módulo de seguridad (320).

3. Procedimiento de gestión según la reivindicación 1, caracterizado porque la segunda área de memoria está situada en otro módulo de seguridad (200).

4. Procedimiento de gestión según la reivindicación 2 ó 3, caracterizado porque la petición de acceso comprende una orden de acción y porque el procedimiento comprende una etapa de ejecución (E20) de dicha acción tras la etapa de transmisión o de almacenamiento.

5. Procedimiento de gestión según la reivindicación 4, caracterizado porque la acción es un bloqueo de dicha aplicación y/o un borrado de datos de dicha aplicación.

6. Procedimiento de gestión según la reivindicación 5, caracterizado porque además comprende una etapa de recepción de una orden de actualización de la aplicación en una tercera área de memoria segura y una etapa de recepción de una orden de transferencia de dichos datos de la segunda área de memoria hacia la tercera área segura.

7. Módulo de seguridad (10, 120, 320) asociado a un terminal móvil, caracterizado porque comprende:

- medios de recepción de un mensaje que contiene una petición de acceso a datos relacionados con una aplicación instalada en el módulo de seguridad, estando almacenados los datos en una primera área de memoria segura del módulo de seguridad, estando cifrado dicho mensaje con una primera clave de gestión,

- medios de obtención de dicha petición mediante descifrado del mensaje por medio de una segunda clave de gestión asociada a la primera clave de gestión,

- medios de lectura de dichos datos,

- medios de cifrado de los datos leídos con la segunda clave de gestión,

- medios de transmisión de los datos cifrados a una segunda área de memoria apta para almacenar los datos cifrados.

8. Terminal caracterizado porque comprende un módulo tal como se define en la reivindicación 7.

9. Producto de programa de ordenador que comprende instrucciones para llevar a la práctica las etapas del procedimiento de gestión según una de las reivindicaciones 1 a 6, cuando es cargado y ejecutado por un procesador.

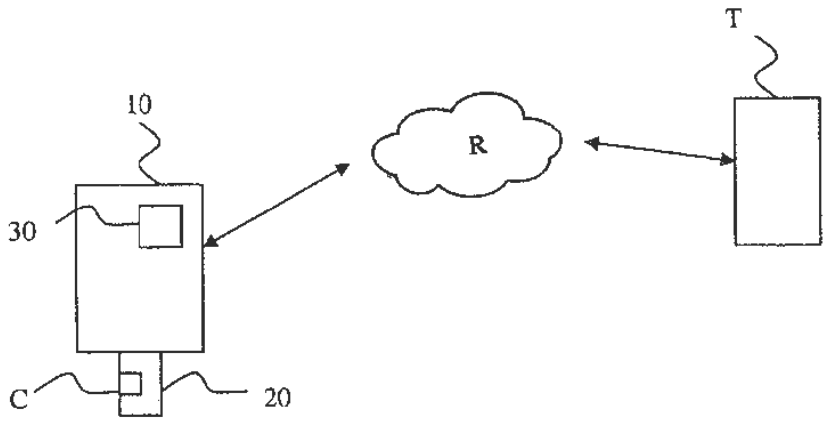

Figura 1

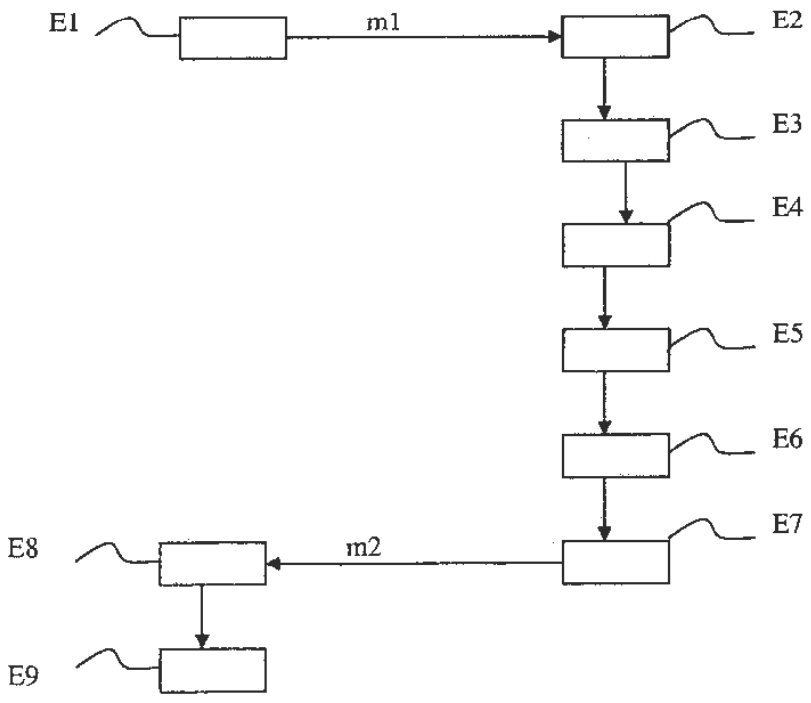

Figura 2

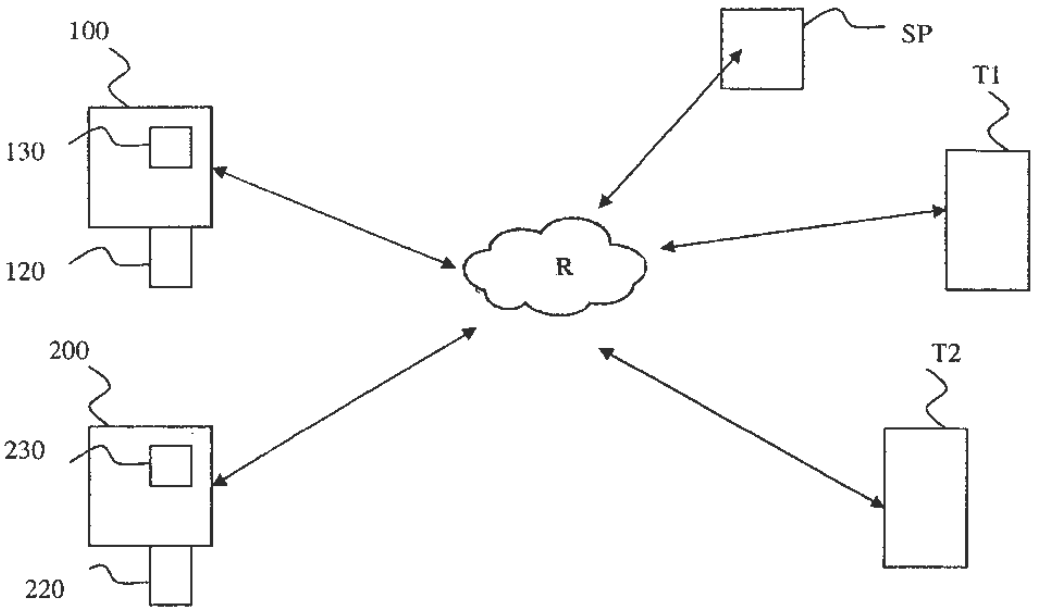

Figura 3

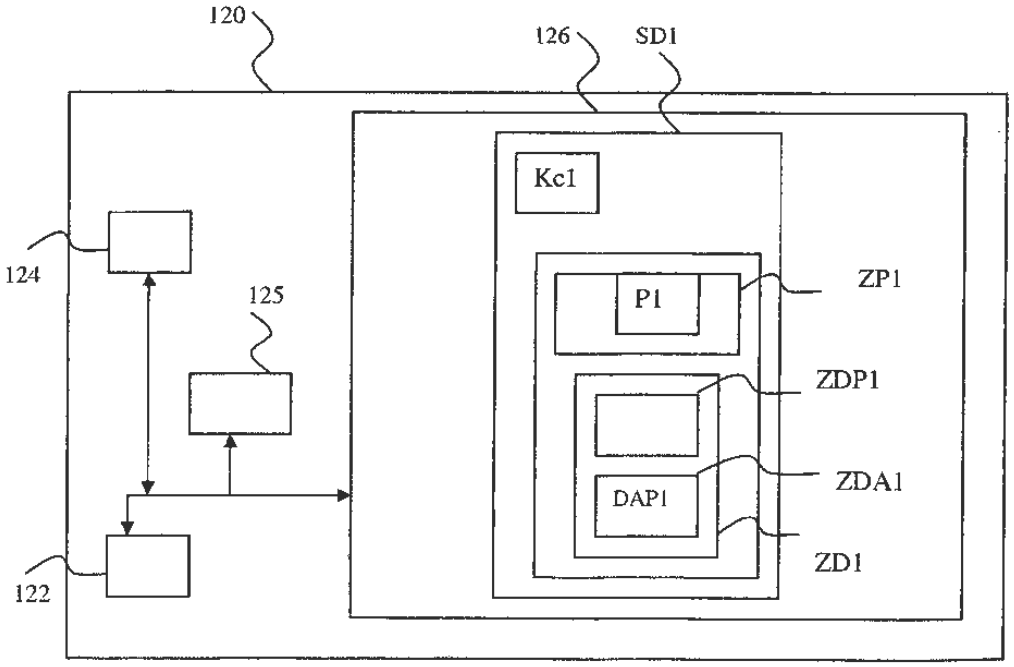

Figura 4

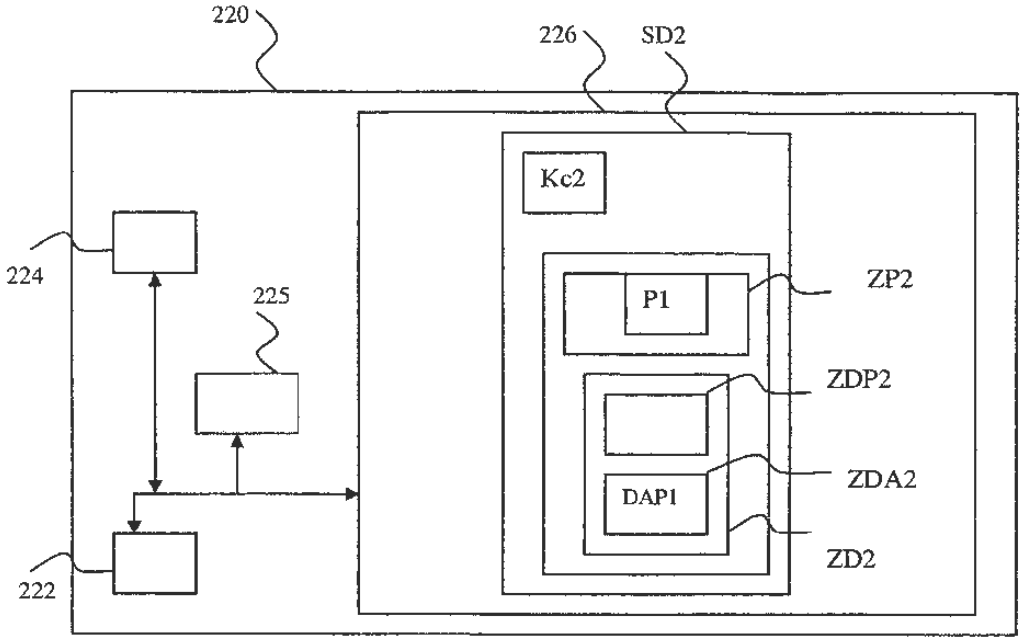

Figura 5

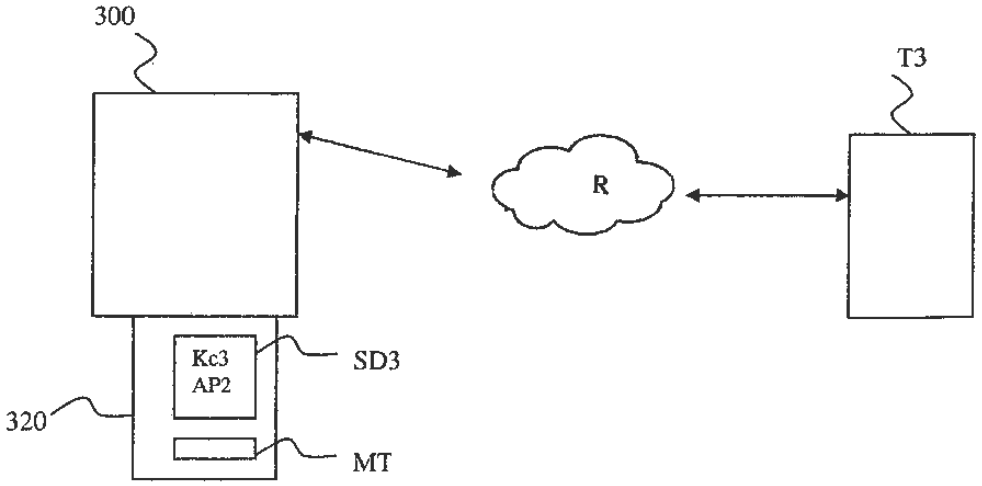

Figura 7

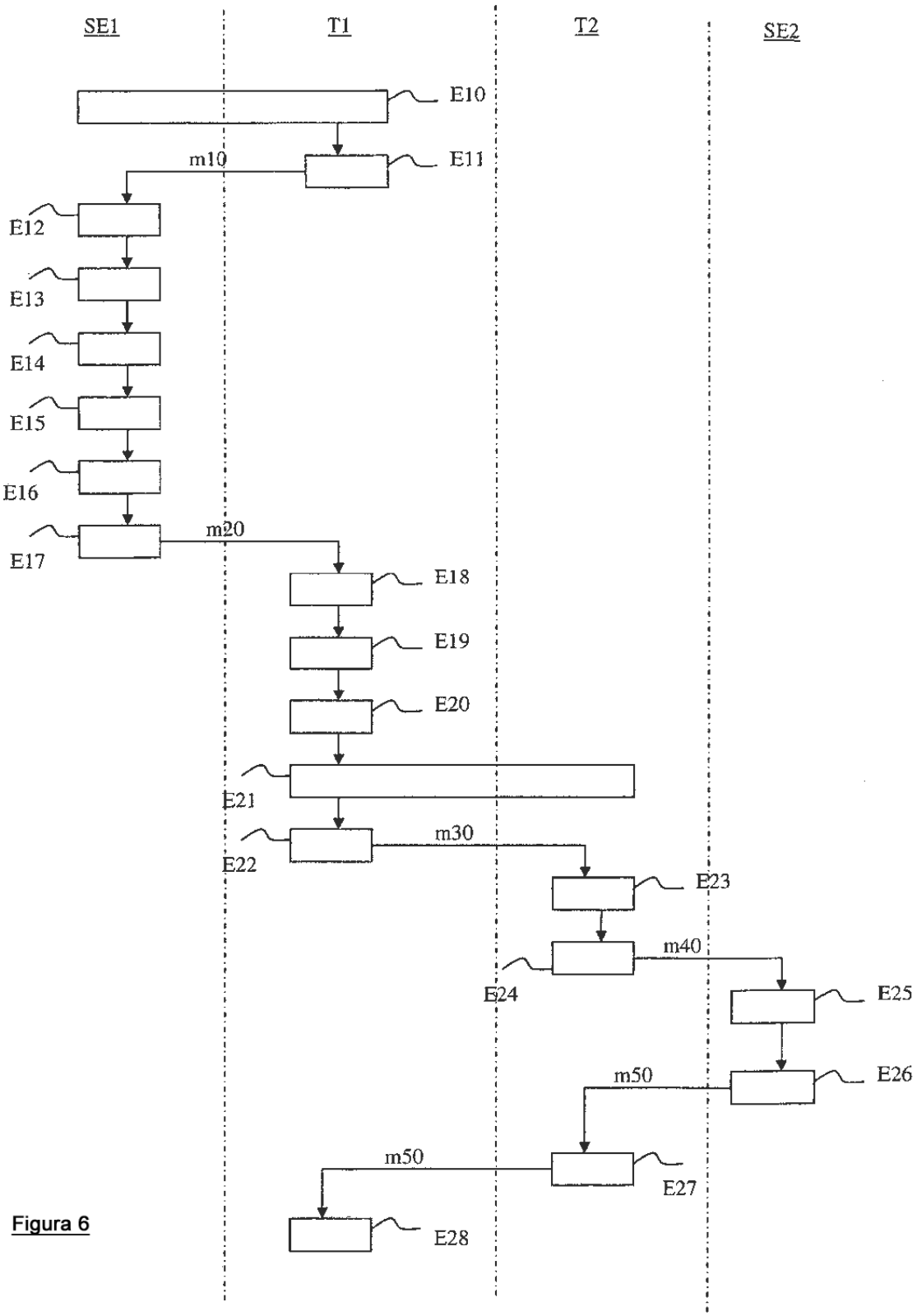
SE1
T1
T2
SE2
E10
m10
E11
E12
E13
E14
E15
E16
E17
m20
E18
E19
E20
E21
E22
m30
E23
m40
E24
E25
m50
E26
m50
E27
E28

Figura 6

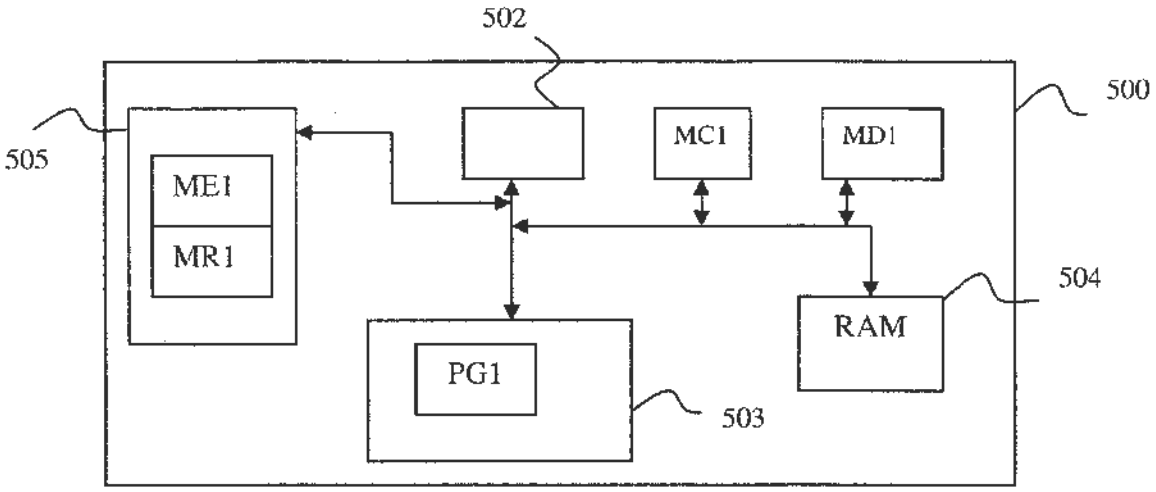

Figura 8

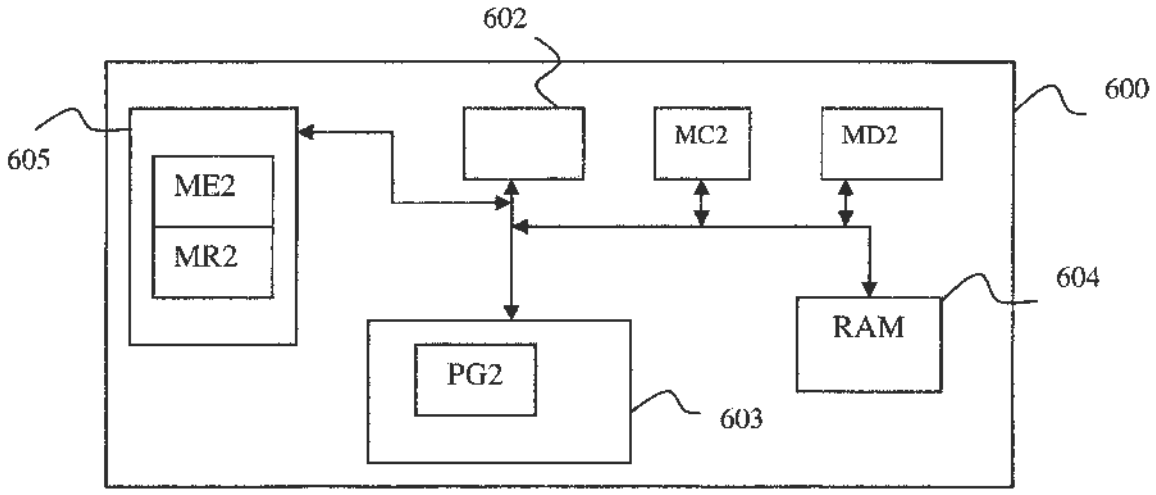

Figura 9