(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 378 252**

(51) Int. CI.:
G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08735872 .7**
(96) Fecha de presentación: **07.04.2008**
(97) Número de publicación de la solicitud: **2149103**
(97) Fecha de publicación de la solicitud: **03.02.2010**

(54) Título: **Método y aparato para proteger la información de "SIMlock" en un dispositivo electrónico**

(30) Prioridad:
20.04.2007 US 913102 P
21.12.2007 US 962356

(45) Fecha de publicación de la mención BOPI:
10.04.2012

(45) Fecha de la publicación del folleto de la patente:
10.04.2012

(73) Titular/es:
Telefonaktiebolaget LM Ericsson (publ)
164 83 Stockholm, SE

(72) Inventor/es:
GEHRMANN, Christian

(74) Agente/Representante:
de Elzaburu Márquez, Alberto

DESCRIPCIÓN

Método y aparato para proteger la información de “SIMlock” en un dispositivo electrónico

ANTECEDENTES

Campo Técnico

La presente invención se refiere generalmente a la seguridad de los dispositivos electrónicos, y particularmente a la información u otros de protección del Subscriber Identity Module Lock (“SIMlock” – “Bloqueo del Módulo de Identidad del Abonado”) que habilita datos en un dispositivo electrónico.

Antecedentes

Los dispositivos electrónicos, particularmente los dispositivos de comunicación de telefonía móvil tales como radioteléfonos móviles, se venden a menudo sujetos a una o más restricciones de uso. Por ejemplo, un dispositivo puede estar restringido para trabajar sólo en ciertos países, sólo con ciertas redes de comunicación y/o proveedores de servicio. Los Subscriber Identity Modules (SIMs – Módulos de Identidad del Abonado) pueden realizar una función clave en hacer que se respeten tales restricciones, ya sea implementadas como hardware en formato de tarjeta, o implementadas en software.

En particular, un dispositivo puede incluir elementos de seguridad que lleven a cabo un “Bloqueo de SIM” (“SIM Lock”), abreviado en esta memoria como “SIMLock” que restringe los SIMs que pueden ser utilizados con el dispositivo. Por ejemplo, el SIMLock de un dispositivo dado puede ser configurado para bloquear el dispositivo para que acepte SIMs sólo de un operador de red específico, o sólo para un país específico. Como otro ejemplo más, algunos dispositivos incluyen SIMLocks que bloquean los dispositivos para SIMs específicos, impidiendo con ello el intercambio de la información de SIM de un dispositivo a otro. Un operador podría, por ejemplo, equipar dispositivos “Premium” o de alta capacidad con ese tipo de SIMLock, para asegurar que cualquier subvención de compra proporcionada por el operador sea recuperada mediante acuerdos de suscripción a largo plazo.

La eliminación, inhabilitación, o cualquier otro modo de saltarse el SIMLock, lo que recibe en general el nombre de fraude de SIMLock, representa un coste significativo para los operadores de red, porque parcial o totalmente les impide la recepción de los ingresos del frente ato de suscripción esperados. Por ello, existe un significativo interés en desarrollar mecanismos de SIMLock que sean difíciles de vencer o de ser saltados de cualquier otro modo, pero que sean prácticos desde la perspectiva económica y de implementación del circuito.

Por ejemplo, Advanced Risc Machines® proporciona una arquitectura de procesamiento seguro comercializada bajo la marca TrustZone®. TrustZone® integra seguridad de hardware y de software, en parte proporcionando entornos de tratamiento dual, que incluyen un entorno de tratamiento seguro, que pueden ser utilizados para verificación de SIM y para el correspondiente tratamiento, y un entorno no seguro, que puede ser utilizado para el procesamiento general del dispositivo. Otros ejemplos de provisiones de entorno de tratamiento seguro con aplicabilidad para tratamiento relacionado con el SIM engloban a Trusted Computing Group™, que es una asociación de varias empresas, que incluyen AMD®, Intel®, HP® y otras. El documento US 2004/0129848 describe un método para asegurar la personalización del SIM y de otros datos en un primer procesador y asegurar la comunicación de los datos del SIM a un segundo procesador.

COMPENDIO

Las enseñanzas de esta memoria presentan un método y aparato para proteger los datos de restricción de utilización que gobiernan el uso de un dispositivo electrónico. Un circuito criptográfico soporta accesos seguros y no seguros. Cuando se accede de manera no segura, se puede operar sólo para verificar los datos de restricción de utilización almacenados y, cuando se accede de manera segura, se puede operar para generar un nuevo código de validación de mensaje para datos de restricción de utilización cambiados, para la subsiguiente validación de esos datos. Los datos de restricción de utilización pueden estar almacenados en una memoria no segura y pueden incluir partes estáticas y dinámicas. Una o más realizaciones incluyen un circuito seguro que indica si el dispositivo ha sido inicializado. El circuito criptográfico emite un código de validación de mensaje para la parte estática que utiliza una clave permanente de dispositivo del circuito seguro sólo si el dispositivo no ha sido inicializado, y emite un código de validación de mensaje para la parte dinámica según sea necesario para soportar cambios autorizados para la parte dinámica.

Ventajosamente, en una o más realizaciones, el circuito criptográfico y el circuito seguro están implementados juntos como partes de un Application Specific Integrated Circuit (ASIC – Circuito Integrado Específico para una Aplicación) o de un System-on-a-Chip (SoC – Sistema-en-un-Microprocesador). Tanto si se implementa de esa manera como si no, el circuito seguro comprende, por ejemplo, una pluralidad de elementos programables una sola vez, tales como fusibles o anti-fusibles. En al menos una realización, la clave permanente del dispositivo es registrada como una clave secreta por medio de un subconjunto de elementos programables una sola vez, y es accesible sólo para el circuito criptográfico. De manera similar, uno o más de los elementos programables una sola vez pueden ser

utilizados como un indicador permanente de si el dispositivo ha sido inicializado, por ejemplo, es un “consumido” durante la inicialización del dispositivo.

Así, en una o más realizaciones, un dispositivo electrónico comprende una primera memoria para guardar datos de restricción de utilización almacenados y un código de validación de mensaje almacenado para la validación de los datos de restricción de utilización, guardando un circuito seguro una clave permanente del dispositivo, y un circuito criptográfico conectado al circuito seguro. El circuito criptográfico es operable cuando no se accede de manera segura, para validar los datos de restricción de utilización almacenados utilizando el código de validación de mensaje y la clave permanente del dispositivo pero no es operable para emitir un nuevo código de validación de mensaje para los datos de restricción de utilización almacenados. Además, el circuito criptográfico es operable, cuando se accede de manera segura, para generar un nuevo código de validación de mensaje utilizando la clave permanente y los datos de restricción de utilización cambiados que han sido generados mediante la modificación autorizada de los datos de restricción de utilización almacenados, y para emitir el nuevo código de validación de mensaje para su almacenamiento en la primera memoria junto con los datos de restricción de utilización cambiados. En al menos una realización tal, la primera memoria ventajosamente comprende una memoria no segura.

Además, en al menos una realización tal, el dispositivo electrónico comprende también un procesador de sistema configurado para operar selectivamente en modos seguro y no seguro. El procesador del sistema es operable para un acceso no seguro al circuito criptográfico para validar los datos de restricción de utilización almacenados, y para un acceso seguro al circuito criptográfico con el fin de obtener el nuevo código de validación del mensaje para los datos de restricción de utilización cambiados. El procesador del sistema en una o más realizaciones también es operable en el modo seguro para generar los datos de restricción de utilización cambiados almacenados en respuesta a ejecutar instrucciones de programa seguras, que pueden estar protegidas en una memoria segura. Como ejemplo no limitativo, el procesador del sistema puede estar configurado al menos en parte de acuerdo con las especificaciones de ARM® TrustZone® o Trusted Computing Group™. De manera más general, el procesador del sistema proporciona dominios de procesamiento seguros y no seguros y es operable para cambiarlos.

Por ejemplo, en al menos una realización, el dispositivo electrónico incluye un temporizador de vigilante de seguridad que reinicia el procesador del sistema a menos que sea oportunamente servido en modo seguro por el procesador del sistema. Complementando tal disposición, el procesador del sistema está configurado para llevar a cabo un reinicio en modo seguro, de manera que el temporizador del vigilante de seguridad fuerce al procesador del sistema a entrar en el modo seguro si no es servido oportunamente por el procesador del sistema.

En una o más realizaciones diferentes, un método de proteger los datos de restricción de utilización que gobiernan el uso de un dispositivo electrónico comprende almacenar los datos de restricción de utilización como datos de restricción de utilización almacenados en una primera memoria del dispositivo electrónico, junto con un código de validación de mensaje almacenado para la validación de los datos de restricción de utilización almacenados, y almacenar una clave permanente del dispositivo en un circuito seguro. El método incluye también, si se está en un modo de operación no seguro, validar los datos de restricción de utilización almacenados utilizando el código de validación de mensaje almacenado y la clave permanente del dispositivo pero sin generar ningún código de validación de mensaje nuevo para los datos de restricción de utilización almacenados. Además, el método incluye, si se está en un modo de operación seguro, generar de manera selectiva un nuevo código de validación de mensaje utilizando la clave permanente y los datos de restricción de utilización cambiados que han sido generados por medio de la modificación autorizada de los datos de restricción de utilización almacenados, y emitir el nuevo código de validación de mensaje para el almacenamiento en la primera memoria junto con los datos de restricción de utilización cambiados.

En al menos una realización tal, el método incluye almacenar los datos de restricción de utilización en el correspondiente código o los correspondientes códigos de validación de mensaje en una memoria no segura. Con o sin ese detalle, no obstante, el método también puede incluir operar en el modo seguro y en el modo no seguro basándose en un procesador de sistema del dispositivo electrónico que cambia dinámicamente entre los modos de operación seguro y no seguro. En tales realizaciones, realizar la modificación autorizada de los datos de restricción de utilización almacenados puede comprender la ejecución por el procesador del sistema de instrucciones de programa seguras, que pueden estar almacenadas en una memoria segura.

Por supuesto, la presente invención no está limitada a las características y ventajas anteriores. En realidad, los expertos en la materia reconocerán características y ventajas adicionales con la lectura de la siguiente descripción detallada, y a la vista de los dibujos que se acompañan.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Fig. 1 es un diagrama de bloques de una realización de un dispositivo electrónico tal como se describe en esta memoria.

La Fig. 2 es un diagrama de flujo lógico de una realización del procesamiento criptográfico tal como se describe en esta memoria para soportar la validación de información.

La Fig. 3 es un diagrama de bloques de una realización de un sistema de inicialización, que puede ser utilizado para inicializar la información de restricción de utilización en un dispositivo electrónico.

Las Figs. 4 y 5 son diagramas de flujo lógicos correspondientes de una realización de procesamiento en soporte del almacenamiento de los datos de restricción de utilización iniciales y generar y almacenar información de validación para esos datos.

La Fig. 6 es un diagrama de una realización de datos almacenados que incluye información de restricción de utilización estática almacenada y un message authentication code (MAC – Código de Validación de Mensaje) almacenado correspondiente.

La Figs. 7 y 8 son diagramas de flujo lógicos correspondientes de una realización de tratamiento en soporte para almacenar datos de restricción de utilización cambiados y generar y almacenar información de validación para esos datos.

La Fig. 9 es un diagrama de una realización de datos almacenados que incluye información de restricción de utilización estática almacenada y un correspondiente MAC almacenado, e incluye además información de restricción de utilización dinámica almacenada y un correspondiente MAC almacenado.

La Fig. 10 es un diagrama de bloques de otra realización de un dispositivo electrónico tal como se describe en esta memoria.

DESCRIPCIÓN DETALLADA

Como ejemplo no limitativo, la Fig. 1 ilustra un dispositivo 10 electrónico que incluye una memoria 12 que guarda datos de restricción de utilización 14 que pretende limitar o restringir de otro modo cómo se utiliza el dispositivo 10. De manera correspondiente, la memoria 12 guarda un message authentication code (MAC – Código de Validación de Mensaje) 16 que se utiliza para validar los datos de restricción de utilización.

Como ejemplo, el MAC 16 puede ser calculado como, por ejemplo, un keyed-hash message authentication code (HMAC – Código de Validación de Mensaje de Clave de Comprobación Aleatoria) basándose en el Secure Hash Algorithm (SHA – Algoritmo de Comprobación Aleatoria Seguro) 256. Se conocen muchas otras funciones de generación de MAC, y pueden ser utilizadas según necesidades o deseos. En líneas generales, el MAC 16 se calcula en función de una clave (secreta) y en una secuencia de datos, es decir, el MAC 16 se define como *f* (clave, secuencia), donde "*f*" es la función de derivación deseada. Así, como procedimiento de almacenamiento inicial, el MAC 16 puede ser calculado para datos de restricción de utilización 14 válidos, conocidos que utilizan una clave secreta. Los datos de restricción de utilización 14 válidos y el correspondiente MAC 16 son almacenados en la memoria 12 y pueden detectarse cambios no autorizados a los datos de restricción de utilización 14 extrayendo los datos de la memoria, calculando un MAC para los datos extraídos que utilizan la misma clave y función de derivación de MAC, y comparando a continuación ese MAC calculado con el MAC 16 almacenado en la memoria 12.

Detectar la falsificación de datos de esta manera es importante en un número de aplicaciones, tales como en las que el dispositivo 10 comprende un radioteléfono celular u otro dispositivo o módulo de comunicación inalámbrico vendido sujeto a restricciones de utilización. En tales realizaciones, los datos de restricción de utilización pueden comprender, como se ha explicado anteriormente en esta memoria, información de Subscriber Identity Module Lock ("SIMLock" – "Bloqueo de Módulo de Identidad de Abonado") que restringe el uso del dispositivo 10.

Ventajosamente, el dispositivo 10 incluye un circuito criptográfico 18 para validar los datos de restricción de utilización 14 almacenados y, cuando sea apropiado, proporcionar un MAC 16 calculado de nuevo, tal como para determinar inicialmente el MAC como parte de la inicialización del dispositivo o para determinar un nuevo MAC para reflejar cambios a los datos de restricción de utilización 14 autorizados. El circuito criptográfico 18 puede ser, por ejemplo, un circuito basado en hardware que tiene estructuras de circuito lógico o si no programadas de otra manera para llevar a cabo las funciones de tratamiento criptográfico deseadas. Como se describe en esta memoria, el circuito criptográfico 18 tiene una conexión 20 a un circuito seguro 22, que guarda de manera segura una clave 24 que es única para el dispositivo 10 en una o más realizaciones, y proporciona un indicador 26 que indica si el dispositivo 10 ha sido inicializado (tal como podría ser realizado por el fabricante del dispositivo durante la configuración inicial o el aprovisionamiento del dispositivo). Así, el circuito seguro 22 puede incluir una pluralidad de elementos one-time programable (OTP – Programables una sola vez) 28, tal como fusibles o antifusibles, para su uso en el almacenamiento permanente de la clave 24 y para ajustar permanentemente el indicador de inicialización 26 después de que el dispositivo 10 ha sido inicializado.

En al menos una realización, la conexión 20 es una conexión directa, o al menos no está disponible para su uso por otras entidades de hardware o de software en el dispositivo 10, lo que significa que sólo el circuito criptográfico 18 tiene acceso a la clave 24, o a una versión encriptada de él. Además, el circuito criptográfico 18 puede estar configurado de tal manera que nunca muestre la clave 24, lo que significa en la práctica que la clave 24 es desconocida y que no se puede descubrir. Además, el circuito criptográfico 18 y el circuito seguro 22 pueden ser implementados como partes de un módulo integrado 30, que puede comprender un Application Specific Circuit

(ASIC – Circuito Específico para una Aplicación), System-on-a-chip (SoC – Sistema en un Microprocesador), u otro circuito empaquetado de ese tipo. Ventajosamente, tal empaquetamiento físico puede estar diseñado para evitar cualquier acceso no destructivo a la interfaz entre el circuito seguro 22 y el circuito criptográfico 24.

Con los detalles no limitativos anteriores en mente, entonces, se comprenderá que el dispositivo 10 en una o más realizaciones comprende una primera memoria, por ejemplo la memoria 12, para guardar los datos de restricción de utilización 14 almacenados y un código de validación de mensaje 16 almacenado para validar los datos de restricción de utilización almacenados. El dispositivo 10 comprende también el circuito seguro 22 que guarda una clave 24 permanente del dispositivo, y el circuito criptográfico 18, que está conectado al circuito seguro 22 y es operable, cuando se accede de manera no segura, para validar los datos de restricción de utilización 14 almacenados utilizando el código de validación de mensaje 16 almacenado y la clave 24 permanente del dispositivo, pero no es operable para emitir un nuevo código de validación de mensaje para los datos de restricción de utilización 14 almacenados. Además, el circuito criptográfico 18 es operable, cuando se accede de manera segura, para generar un nuevo código de validación de mensaje utilizando la clave 24 permanente y los datos de restricción de utilización cambiados que han sido generados mediante la modificación autorizada de los datos de restricción de utilización almacenados, y para emitir el nuevo código de validación de mensaje para el almacenamiento en la primera memoria junto con los datos de restricción de utilización cambiados.

Por ejemplo, uno o más elementos de los datos de restricción de utilización 14 almacenados pueden ser modificados para obtener datos de restricción de utilización cambiados 14', en los que la "primera" marca después del número de referencia textualmente denota datos de utilización. Así, en soporte a procedimientos de modificación autorizados, el circuito criptográfico 18 utiliza la clave 24 para generar un nuevo MAC, es decir, el MAC 16', a partir de los datos de restricción de utilización cambiados 14'. Los datos de restricción de utilización 14 antiguos pueden ser sobre escritos completamente o en parte por los datos de restricción de utilización cambiados 14', y el MAC actualizado 16' puede ser almacenado en la memoria 12 junto con los datos actualizados para una posterior validación de esos datos actualizados. A menos que sea necesario en esta memoria por claridad, los datos de restricción de utilización y el MAC almacenados en la memoria 12 se denotan, respectivamente, utilizando los números de referencia 14 y 16, incluso si representan valores cambiados/actualizados.

Con las protecciones de seguridad frente a modificaciones de datos no autorizadas permitidas por el circuito criptográfico 18 y el circuito seguro 22, la memoria 12 puede ser ventajosamente implementada como memoria no segura, por ejemplo, memoria RÁPIDA u otra memoria no volátil. La utilización de una memoria no segura ahorra dinero y simplifica el diseño, la construcción, las pruebas y la operación del dispositivo 10.

Volviendo al ejemplo de la Fig. 1, se ve que el dispositivo 10 incluye, en una o en más realizaciones, un procesador de sistema 32, que puede estar integrado en el módulo 30 ó no. El procesador de sistema 32 puede tener un "dominio seguro" y un "dominio no seguro", y puede ser configurado, por ejemplo, de acuerdo con estándares o recomendaciones de ARM® TrustZone® o TCG™. En líneas generales, el procesador del sistema 32 está configurado para la operación selectiva en modos seguro y no seguro, y está acoplado al circuito criptográfico 18 a través de uno o más circuitos de bus/interfaz 34. El acoplamiento puede ser indirecto, tal como a través de un circuito de control de acceso 36, que indica/controla si se está accediendo al circuito criptográfico 18 de manera segura o no segura.

Ventajosamente, entonces, el circuito criptográfico 18 está configurado para accesos seguro y no seguro, y el procesador del sistema 32 por lo tanto puede hacer uso del circuito criptográfico 18 en modo seguro y en modo no seguro. No obstante, el circuito criptográfico 18 está, como se ha detallado anteriormente, configurado para comportarse de manera diferente y para proporcionar diferentes funciones, dependiendo de si se accede a él de manera segura o no segura. Esta disposición permite que el circuito criptográfico 18 sea utilizado para operaciones seguras y para operaciones no seguras, sin comprometer la integridad de las operaciones seguras.

En al menos una realización, entonces, el circuito criptográfico 18 está disponible para el procesador del sistema 32 en modo no seguro, para validar los datos de restricción de utilización 14 almacenados, pero no para generar y emitir MACs nuevos que puedan ser utilizados para validar datos de restricción de utilización actualizados. En realidad, el circuito criptográfico 18 está, en una o en más realizaciones, también disponible por medio de un acceso no seguro para un intervalo de tareas de soporte de procesamiento criptográfico que son de ayuda para el dispositivo 10. No obstante, sólo cuando se accede al circuito criptográfico 18 de manera segura está éste disponible para generar nuevos MACs para ser utilizados para la validación de datos de restricción de utilización cambiados.

Así, en una o en más realizaciones, el procesador del sistema 32 está configurado para operar selectivamente en modos seguro y no seguro. El procesador del sistema 32 es operable para un acceso no seguro al circuito criptográfico 18, para validar los datos de restricción de utilización 14 almacenados, y es operable en el modo seguro para generar los datos de restricción de utilización cambiados en respuesta a la ejecución de instrucciones de programa seguras y a un acceso seguro al circuito criptográfico para obtener el nuevo código de validación de mensaje para los datos de restricción de utilización cambiados. En al menos una realización tal, un operador de red o agente de proveedor de servicios tiene un sistema de ordenador que se acopla al dispositivo 10 y que está configurado con los códigos de validación adecuados para controlar o en su lugar iniciar el cambio de los datos de

restricción de utilización. En otros casos, el dispositivo 10 puede, por medio del procesador del sistema 32 y de instrucciones de programa seguras, ser configurado para permitir cambios over-the-air (OTA – En el aire), tal como parte de un proceso de re-aprovisionamiento autorizado.

Así, el dispositivo 10 en una o en más realizaciones incluye una memoria de programa 38 segura, que puede estar integrada con el procesador del sistema 32 ó no, pero que generalmente está protegida dentro del dominio seguro del procesador del sistema 32. Las instrucciones de programa que soportan el cambio de los datos de restricción de utilización almacenados por lo tanto pueden ser almacenados se manera segura en la memoria de programa 38 segura, para que el procesador del sistema 32 acceda a ellos como parte de procedimientos de actualización autorizados.

La Fig. 2 ilustra un ejemplo de acondicionamiento del comportamiento del circuito criptográfico 18 acerca del tipo de acceso. Tal procesamiento puede ser implementado por medio de circuitos lógicos, firmware o mediante algún otro mecanismo dentro del circuito criptográfico 18. En cualquier caso, el procesamiento ilustrado empieza con el acceso al circuito criptográfico 18. Así, el circuito criptográfico 18 determina si el acceso es seguro o no seguro (Bloque 100). Si el acceso es no seguro, el circuito criptográfico 18 llevará a cabo, con respecto a los datos de restricción de utilización 14 almacenados, sólo funciones de verificación (validación) (Bloque 102). Más particularmente, los datos de restricción 14 almacenados y el correspondiente MAC 16 almacenado pueden ser leídos por (o si no proporcionados a) el circuito criptográfico 18, en cuyo caso el circuito criptográfico 18 subsiguientemente emite una indicación de si los datos de restricción 14 almacenados son o no auténticos. No obstante, el circuito criptográfico 18 no generará ni emitirá nuevos MACs para datos de restricción de utilización cambiados cuando se accede a ellos de manera no segura.

Por el contrario, si el acceso es seguro, el circuito criptográfico 18 lleva a cabo La validación y/o la generación de nuevos MACs para datos de restricción almacenados (Bloque 104). Por ejemplo, el procesador del sistema 32 puede acceder al circuito criptográfico 18 de manera segura, y se le pueden proporcionar datos de restricción de utilización cambiados, mediante una orden u otra indicación de que se va a generar un nuevo MAC para los datos de restricción de utilización cambiados utilizando la clave 24 secreta. En general, tales acciones pueden ser llevadas a cabo “según necesidades” o “mediante una orden”. Además, en líneas generales, el circuito criptográfico 18 en una o más realizaciones puede reconocer un número de órdenes y/o puede estar configurado para llevar a cabo un tratamiento definido dependiendo de en qué modo se accede y de qué datos se le proporcionan.

Por supuesto, como se ha explicado anteriormente, el alcance o la naturaleza del soporte criptográfico proporcionado por el circuito criptográfico 18 puede, además, estar ligado al tipo de acceso (seguro o no seguro), estar ligado a si el dispositivo 10 ha sido inicializado. Como se ha observado, el indicador 26, que puede ser un fusible/antifusible y otro tipo de OTP, se utiliza como un indicador permanente o seguro del estado de inicialización del dispositivo.

La Fig. 3 ilustra a modo de ejemplo no limitativo un sistema de inicialización 40, que puede comprender un sistema de fabricación/inicialización que opera de manera segura en el fabricante de un dispositivo. El sistema de inicialización 40 tiene acceso a una base de datos 42 ó a otro almacén de datos que incluye información de restricción de utilización por defecto. Como ejemplo, el vendedor del dispositivo que opera el dispositivo de inicialización 40 puede proporcionar dispositivos 10 a más de un operador de red, y/o puede proporcionar una variedad de tipos de dispositivos, por ejemplo, desde módulos de comunicación simples hasta sofisticados teléfonos inteligentes. En cualquier caso, la base de datos 42 puede incluir diferentes conjuntos de restricciones de utilización por defecto para operadores de red particulares y/o para modelos de dispositivo particulares.

Un dispositivo 10 dado, puede de este modo ser cargado con datos de restricción de utilización por defecto como parte del proceso de inicialización. En una o más realizaciones, los datos de restricción por defecto comprenden, por ejemplo, datos de validación estáticos que definen valores de clave de palabra de paso que son utilizados para autorizar cambios en las restricciones de utilización, y datos dinámicos que comprenden las reglas o ajustes que definen tales restricciones. Generalmente, no se pretende que los datos estáticos cambien en toda la vida del dispositivo 10, y se pretende que los datos dinámicos cambien sólo bajo condiciones de operación segura mediante una adecuada autorización.

La Fig. 4 ilustra un ejemplo de procesamiento, desde la perspectiva del dispositivo 10. El procesamiento empieza con que el dispositivo 10 recibe datos de restricción de utilización iniciales y cualquier dato de orden/configuración relacionado para llevar a cabo una inicialización del dispositivo autorizada (Bloque 110). El procesamiento continúa con el acceso de manera segura al circuito criptográfico 18, para solicitar o si no obtener un MAC para los datos de restricción de utilización iniciales (Bloque 112). (El circuito criptográfico 18 genera ese MAC procesando los datos de restricción de utilización iniciales, por ejemplo, codificándolos, utilizando la clave 24 secreta, que incluye utilizar la clave 24 directamente o derivando una clave de la clave 24 como podría hacerse para una mayor seguridad.

El procesador del sistema 32 u otra entidad dentro del dispositivo 10 ó del sistema de inicialización 40 recibe el MAC nuevamente generado y hace que los datos de restricción de utilización iniciales y el MAC se almacenen en la memoria 12 como los datos de restricción de utilización 14 almacenados y el correspondiente MAC almacenado

(Bloque 114). A continuación, el dispositivo 10 ó el sistema de inicialización 40 hacen que una señal de programación sea aplicada al circuito seguro 22, para ajustar de manera permanente el indicador de inicialización 26, para indicar que el dispositivo 10 ha sido inicializado (Bloque 116). Ventajosamente, esa indicación se utiliza en una o en más realizaciones para impedir que el circuito criptográfico 18 calcule nunca un nuevo MAC para una o más partes de los datos de restricción de utilización iniciales que acaban de ser almacenados en la memoria 12. Esta disposición significa que esas una o más partes de los propios datos de restricción de utilización iniciales no pueden ser alterado o alterados y validado o validados de nuevo una vez que el dispositivo 10 ha sido inicializado. En al menos una realización, entonces, los datos de restricción de utilización iniciales comprenden valores de validación estáticos para los cuales el dispositivo 10 no calculará un nuevo MAC una vez que el indicador de inicialización 26 se ha establecido, y valores dinámicos (reglas o ajustes), que pueden ser cambiados más tarde y para los cuales pueden calcularse nuevos valores de MAC, pero sólo mediante autorización frente a los valores de autorización estáticos de acuerdo con operaciones de procesamiento seguras.

La Fig. 5 ilustra el efecto de esa restricción en el procesamiento mediante el circuito criptográfico 18. La Fig. 5 más particularmente representa el procesamiento llevado a cabo por el circuito criptográfico 18 dentro del contexto de procesamiento de inicialización del Bloque 112 de la Fig. 4. Así, el procesamiento ilustrado empieza con que el circuito criptográfico 18 recibe los datos de restricción de utilización iniciales (por ejemplo, directa o indirectamente desde el sistema de inicialización 40), y una solicitud o indicación adjunta de que el circuito criptográfico 18 debería generar y emitir un MAC para las datos de restricción de utilización iniciales (Bloque 120). El circuito criptográfico 18 por lo tanto comprueba si el indicador 26 indica que el dispositivo 10 ha sido inicializado (Bloque 122). Si lo ha sido, el circuito criptográfico 18 no generará el MAC. Para hacer que se vea ese fallo, en al menos una realización, el circuito criptográfico 18 devuelve una información de error u otra información (Bloque 124).

Si el indicador 26 no indica que el dispositivo 10 ha sido inicializado, el circuito criptográfico 18 obtiene la clave 24 en formato sin codificar o en formato codificado a partir del circuito seguro 22 por medio de la conexión 20 (Etapa 126). El circuito criptográfico 18 genera a continuación el nuevo MAC, por ejemplo como (clave 24, datos de restricción de utilización iniciales) (Bloque 128), y emite el nuevo MAC para su almacenamiento en la memoria 12 (Bloque 130), tal como puede realizarse bajo el control del procesador del sistema 32. No obstante, se contempla en esta memoria que al menos una realización del circuito criptográfico 18 incluye al menos una capacidad de interconexión de memoria limitada, lo que significa que el circuito criptográfico 18 puede ser capaz de escribir MACs en la memoria 12 y/o de obtener datos de utilización 14 almacenados y MACs 16 almacenados de la memoria 12.

La Fig. 6 ilustra el almacenamiento de datos para la memoria 12 como resultado del tratamiento de inicialización anterior. Se ve que los datos de restricción de utilización 14 almacenados comprenden “datos de restricción de utilización estáticos” 44 almacenados con la connotación de que son datos de restricción de utilización por defecto o de inicio cargados en el dispositivo 10 como parte de la inicialización autorizada del dispositivo 10. De manera más pertinente, el término “datos de restricción de utilización estáticos” tiene la connotación de los datos de restricción de utilización que están previstos para que no cambien nunca en toda la vida del dispositivo 10. De manera correspondiente, el MAC 16 almacenado comprende un “MAC de datos estáticos almacenado 46”, que está previsto para su uso subsiguiente en validar los datos de utilización estáticos almacenados 44.

La Fig. 7 ilustra el procesamiento mediante, por ejemplo, el procesador del sistema 32, para llevar a cabo cambios autorizados a las restricciones de utilización del dispositivo. El procesamiento empieza cuando el procesador del sistema 32 determina si el cambio que se intenta realizar está autorizado (Bloque 140). Esto puede ser llevado a cabo de un modo seguro, basándose en que el procesador del sistema 32 verifica las claves/códigos de paso, u otros, que pueden estar almacenados en formato codificado en los datos de restricción de utilización estáticos 44, o las palabras de paso/códigos de paso codificados de un solo sentido están almacenados en los datos de restricción de utilización estáticos 44. Si el cambio no es parte del tratamiento autorizado, el procesador del sistema impide los cambios y los aborta (Bloque 142).

En al menos una realización, los propios datos de restricción de utilización estáticos 44 nunca se cambian. Por ejemplo, los datos de restricción de utilización estáticos 44 comprenden valores de claves de paso codificadas de un solo sentido que se utilizan como valores de autorización para cambiar los datos de restricción de utilización dinámicos, los cuales, pueden estar protegidos mediante un MAC diferente. En este caso, los datos de restricción de utilización dinámicos pueden entenderse como datos que contienen las reglas que determina el bloqueo a un cierto SIM y/o red, etc. Por ello, después de una autorización con éxito del usuario, al usuario puede permitírsele cambiar uno o más ajustes definidos por los datos de restricción de utilización dinámicos, pero los datos de autorización subyacentes incorporados en los datos de restricción de utilización estáticos 44 no cambian, por ejemplo las claves de bloqueo de SIM estáticas utilizadas para autorizar cambios del bloqueo de SIM no cambiarían.

Por otro lado, si el cambio es autorizado, el procesador del sistema 32 genera los datos de restricción de utilización cambiados. Por ejemplo, después de que el contrato de servicio inicial expira para el dispositivo 10, su propietario puede desear utilizar el dispositivo con otro proveedor de servicios, o al menos tener la opción de utilizarlo con otra red distinta de la red del proveedor de servicios original. Así, utilizando procedimientos autorizados, pueden llevarse a cabo cambios a los datos de restricción de utilización dinámicos. Esta operación puede entenderse como generadora o si no receptora de datos de restricción de utilización cambiados (Bloque 144). En al menos una

realización, los “datos de restricción de utilización cambiados” representan cambios o actualizaciones a los ajustes llevados a cabo o si no establecidos por los datos de restricción de utilización dinámicos. Tales datos se proporcionan al circuito criptográfico 18 por medio de una solicitud de acceso seguro, junto con cualquier solicitud adjunta requerida de generación de un nuevo MAC para esos datos (Bloque 146). En respuesta, el circuito criptográfico 18 genera un nuevo MAC a partir de los datos de restricción de utilización cambiados. El procesador del sistema recibe el nuevo MAC del circuito criptográfico 18 (Bloque 148) y almacena los datos de restricción de utilización cambiados y el nuevo MAC correspondiente en la memoria 12 (Bloque 150).

La Fig. 8 representa una realización de procesamiento mediante el circuito criptográfico 18 en soporte del procesamiento global anterior. Particularmente, la Fig. 8 representa una realización de procesamiento mediante circuito criptográfico llevada a cabo en respuesta a que el circuito criptográfico 18 recibe los datos de restricción de utilización cambiados por medio de un acceso seguro, como se describió en el Bloque 146 de la Fig. 7.

El procesamiento de la Fig. 8 empieza entonces con que el circuito criptográfico 18 recibe de manera segura los datos de restricción de utilización cambiados y cualquier solicitud o indicación adjunta de que se desea un nuevo MAC para tales datos (Bloque 152). El procesamiento continúa con que el circuito criptográfico 18 obtiene la clave 24 permanente del circuito seguro 22 (por medio de la conexión 20) (Bloque 154), y genera el nuevo MAC de acuerdo con ella (Bloque 156), por ejemplo el nuevo MAC = *g*(clave 24, datos de restricción de utilización cambiados), donde *g*(•) indica una función de generación de MAC que preferiblemente es diferente de la función de generación de MAC (•) utilizada en asociación con la generación de MAC para los datos de restricción de utilización estáticos 44. El procesamiento continúa con que el circuito criptográfico emite el nuevo MAC para su almacenamiento en la memoria 12, junto con los datos de restricción de utilización cambiados.

La Fig. 9 ilustra una realización de los datos y de la disposición de MAC que salen del anterior procesamiento. Como se ilustra, después de iniciar una modificación autorizada de las restricciones de utilización del dispositivo, los datos de restricción de utilización realmente comprenden dos partes: los datos de restricción de utilización estáticos 44 almacenados, que fueron cargados en el dispositivo 10 como parte de su inicialización (por ejemplo, en la fábrica), y los datos de restricción de utilización dinámicos 48 almacenados que fueron generados dentro o proporcionados de otro modo al dispositivo 10 como parte de un procedimiento autorizado para modificar las restricciones de utilización del dispositivo. De manera correspondiente, el MAC 16 realmente comprende un primer MAC para la validación de los datos de restricción de utilización estáticos 44 almacenados, es decir, el MAC 16 de los datos estáticos almacenados, y un segundo MAC para la validación de los datos de restricción de utilización dinámicos 48 almacenados, es decir, el MAC dinámico 50 almacenado. Por ejemplo, como se ha observado anteriormente, el MAC 46 puede obtenerse como (clave 24, datos de restricción de utilización estáticos) y el MAC 50 puede obtenerse como *g*(clave 24, datos de restricción de utilización cambiados).

Con la Fig. 9 en mente, entonces, debe entenderse que los datos de restricción de utilización 14 almacenados pueden comprender una parte estática 44 y una parte dinámica 48 y el MAC 16 almacenado de manera correspondiente comprende un primer MAC almacenado para la validación de la parte estática y un segundo MAC 50 almacenado para la validación de la parte dinámica. En tales contextos, una realización del circuito criptográfico 18 es operable, cuando se accede de manera segura, para generar que se emita un nuevo MAC para la parte estática de los datos de restricción de utilización 14 almacenados para su almacenamiento en la primera memoria como el primer MAC 46 almacenado sólo si el indicador 26 indica que el dispositivo 10 no ha sido inicializado. Además, el circuito criptográfico 18 en tal realización es operable, cuando se accede de manera segura, para generar que se emita un nuevo MAC para la parte dinámica de los datos de restricción de utilización 14 almacenados para su almacenamiento en la primera memoria como el segundo MAC 50 almacenado en respuesta a órdenes seguras proporcionadas a él por medio del acceso seguro o por el procesador del sistema 32.

Esta disposición permite que el dispositivo sea inicializado con códigos/claves de validación para su almacenamiento como datos de restricción de utilización estáticos 44 almacenados y como restricciones de utilización iniciales como las definidas por los datos de restricción de utilización dinámicos 48 almacenados. El correspondiente MAC 46 de los datos estáticos almacenados y el MAC 50 de los datos dinámicos almacenados son almacenados para los datos de restricción de utilización estáticos y dinámicos 44 y 48. Como se ha observado, consumiendo o estableciendo de otro modo el indicador de inicialización evita el cálculo de un nuevo MAC para los datos de restricción de utilización estáticos 44 almacenados, lo que significa que los cambios de pos-inicialización a los datos de restricción de utilización estáticos 44 almacenados no pueden ser validados. No obstante, con una adecuada verificación de la autorización frente a los datos de restricción de utilización estáticos 44 almacenados, puede conseguirse que el circuito criptográfico 18 calcule un nuevo MAC para datos de restricción de utilización (dinámicos) cambiados. Esa funcionalidad permite que se realicen cambios dinámicos en los datos de restricción de utilización dinámicos para su almacenamiento como los datos de restricción de utilización dinámicos 48 almacenados, y permite que se calcule un MAC actualizado de manera correspondiente y que sea almacenado como el MAC 50 de datos dinámicos almacenados. Este procesamiento permite por consiguiente una posterior validación de cambios autorizados realizados en la parte dinámica de los datos de restricción de utilización 14 almacenados.

Volviendo a otros aspectos del dispositivo 10, la Fig. 10 proporciona detalles de ejemplo para otra realización del dispositivo 10. Además de los elementos ilustrados previamente, el dispositivo 10 ilustrado incluye un circuito

temporizador 60 de vigilante de seguridad para asegurar una entrada periódica del procesador del sistema 32 en modo seguro, un circuito de puente 52 y un circuito de control de acceso 64 que funcionan como el circuito de acceso 36 ilustrado anteriormente, un RAM 66 seguro y una interfaz de memoria externa 68 para interconectarse con realizaciones de memoria externa de la memoria 12. Además, la memoria 12 puede incluir datos adicionales 70, tales como datos de configuración, datos de usuario, etc., y el circuito seguro 22 también puede incluir elementos OTP adicionales u otro almacenamiento (memoria) para guardar datos de configuración 72 de seguridad adicionales y/u otros datos de configuración 74. Además, el dispositivo 10 incluye una tarjeta de SIM 76 ó al menos una interfaz de circuito de tarjeta de SIM 78, para recibir y comunicarse con una tarjeta de SIM 76.

En al menos una realización del dispositivo 10 ilustrado, el procesador del sistema 32 está configurado para iniciarse en el modo seguro en respuesta a un reinicio, y el circuito temporizador del vigilante de seguridad 60 está configurado para llevar a cabo un reinicio al procesador del sistema 32 a menos que el procesador del sistema 32 que opera en el modo seguro le preste servicio periódicamente. Esto es, a menos que el procesador del sistema entre en el modo seguro y proporcione servicio (reinicie) al circuito temporizador del vigilante de seguridad 60 antes de que el intervalo temporizado del vigilante expire, el circuito temporizador del vigilante de seguridad 60 impone una señal de reinicio para el procesador del sistema 32, haciendo que se re arranque/reinicie y entre en el modo seguro. En al menos una realización tal, el procesador del sistema 32 está configurado para iniciarse en el modo seguro en respuesta a un reinicio y para proporcionar servicio oportunamente al temporizador del vigilante de seguridad 60, al menos en parte validando los datos de restricción de utilización 14 almacenados y comprobándolos frente a ajustes de Subscriber Identity Module (SIM – Módulo de Identidad del Abonado) para el dispositivo electrónico (que son guardados, por ejemplo, en el SIM 76), donde el temporizador del vigilante de seguridad 60 está configurado para llevar a cabo un reinicio el procesador del sistema 32 a menos que el procesador del sistema 32 que opera en el modo seguro le preste servicio oportunamente.

De manera correspondiente, el procesador del sistema 32 puede estar configurado para, como una parte definida de su procesamiento en modo seguro, utilizar el circuito criptográfico 18 para la validación de los datos de restricción de utilización estáticos 44 almacenados y/o los datos de restricción de utilización dinámicos 48 almacenados. Para ello, el circuito criptográfico 18 está provisto (o lee) los datos de restricción de utilización estáticos 44 almacenados y el correspondiente MAC de los datos estáticos 46 almacenados, y está provisto de (o lee) los datos de restricción de utilización dinámicos 48 almacenados y el correspondiente MAC de los datos dinámicos 50 almacenados. El circuito criptográfico 18 valida los datos de restricción de utilización estáticos 44 almacenados calculando un MAC como (clave 24, datos de restricción de utilización estáticos 44 almacenados), y comproba ndo si el resultado es igual al MAC de los datos estáticos 46 almacenado. Asimismo, valida los datos de restricción de utilización dinámicos 48 almacenados calculando un MAC como (clave 24, datos de restricción de utilización dinámicos 48 almacenados), y comprobando si ese resultado es igual al MAC de los datos dinámicos 50 almacenado.

Debido a que tal validación puede hacerse una parte requerida del procesamiento del dominio seguro, y debido a que el circuito temporizador del vigilante de seguridad 60 garantiza que el procesador del sistema 32 es reiniciado en el modo seguro, el dispositivo 10 puede ser forzado a verificar periódicamente la autenticidad de sus datos de restricción de utilización 14 almacenados (y forzado a comprobar los datos de restricción de utilización verificados frente al SIM actualmente conectado al dispositivo 10). Así, incluso si un cambio no autorizado tiene éxito en activar temporalmente el dispositivo 10 en violación de sus restricciones de utilización, esa condición tiene una vida corta y es detectada mediante el temporizado o forzado reinicio del procesador del sistema 32 en el modo seguro.

En al menos una realización, los datos de restricción de utilización 14 almacenados comprende información del SIMLock, que puede incluir partes estáticas y dinámicas. Como antes, el circuito criptográfico 18 está configurado para generar y emitir un primer MAC sólo para la parte estática como parte del inicio seguro del dispositivo 10, de manera que ningún cambio a la parte estática será nunca validado por el circuito criptográfico 18. El circuito criptográfico 18 está también configurado como parte del cambio de la parte dinámica autorizada, para generar y emitir un nuevo MAC para la parte dinámica, con el fin de permitir una subsiguiente validación de cambios autorizados a la parte dinámica (de los datos de restricción de utilización 14 almacenados).

En un ejemplo más detallado de la protección del SIMLock anterior, resulta útil reiterar que la información del SIMLock está prevista para restringir la utilización del dispositivo 10 a características y privilegios contratados o pagados. Por ejemplo, la información del SIMLock puede estar configurada para asegurar que el dispositivo 10 permanece bloqueado a una red particular (o subconjunto de red, proveedor de servicio, corporación o incluso SIM individual) hasta que sea desbloqueado de una manera autorizada. La información del SIMLock representa por consiguiente una personalización de las características permitidas para el dispositivo 10 con respecto a su comprador o usuario.

Así, el dispositivo 10 puede estar configurado para leer información de la tarjeta de SIM 76 durante el inicio o en otros momentos, y asegurar que tal información comprueba frente a las limitaciones de utilización representadas por la información del SIMLock. Por supuesto, el circuito criptográfico 18 puede en primer lugar ser utilizado para validar la información del SIMLock, y para apagar o llevar a cabo otra acción controlada cuando suceden fallos de validación. Por ejemplo, el dispositivo 10 puede entrar en “estado de servicio limitado” en el cual sólo pueden intentarse llamadas de emergencia.

En al menos otra realización, existen cinco categorías de personalización que pueden estar representadas en y estar controladas por la información del SIMLock almacenada como los datos de restricción de utilización 14 en la memoria 12. Particularmente, un número de “claves de control” pueden estar almacenadas en formato codificado o aleatoriamente codificado de un solo sentido dentro de los datos de restricción de utilización estáticos 44 almacenados. Cambiar una restricción de utilización particular requiere por consiguiente que un usuario autorice frente a la correspondiente clave de control.

Ejemplos no limitativos de tales claves de control incluyen una “Network Control Key” (NCK – Clave de Control de Red) dentro de una categoría de Red. En una categoría de subconjunto de Red, la información puede incluir una “Network Subset Control Key” (NSCK – Clave de Control de Subconjunto de Red). En una categoría de Service Provider (SP – Proveedor de Servicio), la información puede incluir una “Service Provider Control Key” (SPCK – Clave de Control de Proveedor de Servicio). En una categoría Corporativa, la información puede incluir una “Corporate Control Key” (CCK – Clave de Control Corporativa). Finalmente, en una categoría de SIM/USIM, la información puede incluir una “Personalization Control Key (PCK – Clave de Control de Personalización). (Por consiguiente, en al menos una realización, los datos de restricción de utilización estáticos 44 almacenados comprenden claves de autorización/códigos de paso para hacer cambios de restricción, y los datos de restricción de utilización dinámicos 48 comprenden ajustes de restricción que pueden ser modificados sujetos a autorización.)

Las categorías de personalización anteriores son independientes en tanto en cuanto cada categoría puede ser activada o desactivada independientemente del estatus de las otras. Esta disposición permite que el dispositivo 10 sea inicialmente (o posteriormente) personalizado a una red, un subconjunto de red, un SP, una cuenta Corporativa, un SIM/USIM o cualquier combinación de los mismos. Asegurando que todas esas limitaciones basadas en clave sean forzadas, la información del SIMLock proporciona una base para comparar los diferentes posibles ajustes de bloqueo con un “campo de identidad de abonado”, por ejemplo, el International Mobile Station Identifier (IMSI – Identificador de Estación de Telefonía Móvil Internacional), que está almacenado de manera segura en la tarjeta de SIM 76. (Debe observarse que la tarjeta de SIM 76 se ilustra y se explica en esta memoria por simplicidad, pero la misma funcionalidad aplica si un SIM basado en software está instalado en el dispositivo 10.)

Para el contexto anterior, protección de la información del SIMLock consiste en tres partes principales: proteger los códigos de desbloqueo del SIMLock, es decir los valores de clave estática o de código de paso para autorizar cambios; proteger los ajustes del SIMLock configurados, es decir, los ajustes de restricción dinámica; y proteger frente a una reprogramación o alteración no autorizada de nada de la información de SIMLock estática y dinámica. El circuito criptográfico 18, que incluye sus restricciones de operación almacenada/no segura y su uso de una única clave 24 de dispositivo al que se accede de manera segura en el circuito almacenado 22, asegura las protecciones anteriores en una disposición que proporciona una seguridad robusta, de implementación económica, diseño simplificado y ventajosamente uso dual (acceso seguro/no seguro) del circuito criptográfico 18.

Las enseñanzas de esta memoria proporcionan así un aparato y un método para proteger los datos de restricción de utilización que gobierna la utilización de un dispositivo electrónico. En una o más realizaciones, un método comprende configurar un circuito criptográfico del dispositivo electrónico para llevar a cabo sólo validación de los datos de restricción de utilización almacenados recibidos de una memoria del dispositivo electrónico si al circuito criptográfico no se ha accedido de manera segura, y llevar a cabo la generación de un nuevo código de validación de mensaje para una subsiguiente validación de los datos de restricción de utilización cambiados si al circuito criptográfico se ha accedido de manera segura y se le envía una orden para llevar a cabo la citada generación del nuevo código de validación de mensaje.

El método puede también comprender almacenar de manera segura una clave permanente de dispositivo en un circuito no seguro y conectar el circuito seguro al circuito criptográfico. Configurar el circuito criptográfico del dispositivo electrónico para llevar a cabo sólo la validación de los datos de restricción de utilización almacenados si al circuito criptográfico se ha accedido de manera no segura puede comprender configurar el circuito criptográfico para, en el caso de accesos no seguros, leer los datos de restricción de utilización almacenados y un MAC almacenado correspondiente, leer la clave permanente del dispositivo, calcular un MAC a partir de los datos de restricción de utilización almacenados utilizando la clave permanente del dispositivo, y comparar el MAC calculado con los datos de restricción de utilización almacenados, mientras que se impide el que se emita de alguna manera el MAC calculado.

Además, configurar el circuito criptográfico del dispositivo electrónico para llevar a cabo la generación del nuevo MAC si al circuito criptográfico se ha accedido de manera segura y si está gobernado para llevar a cabo la citada generación del nuevo MAC puede comprender configurar el circuito criptográfico para responder a una o más órdenes de generación si se ha accedo de manera segura. Por ejemplo, el circuito criptográfico puede estar configurado para responder a la orden apropiada leyendo la clave permanente del dispositivo, calculando el nuevo MAC a partir de los datos de restricción de utilización cambiados utilizando la clave permanente del dispositivo, y mostrando el nuevo MAC para almacenarlo junto con los datos de restricción de utilización cambiados.

Por supuesto, resultará evidente para los expertos en la materia que la descripción anterior y los dibujos que se acompañan representan ejemplos no limitativos de los métodos y aparatos descritos en esta memoria. De esta

manera, la presente invención no está limitada por la descripción anterior y los dibujos que se acompañan. Por el contrario, la presente invención está limitada sólo por las siguientes reivindicaciones y sus equivalentes legales.

REIVINDICACIONES

1. Un dispositivo electrónico que comprende:

una memoria no segura (12) para guardar datos de restricción de utilización (14) almacenados y un código (16) de validación de mensaje para la validación de los datos de restricción de utilización almacenados;

un circuito seguro (22) que guarda una clave (24) permanente;

un circuito criptográfico (18) conectado al circuito seguro mediante una conexión segura (20) operable, cuando no se ha accedido de manera segura a través de una interfaz de bus (34), para validar los datos de restricción de utilización almacenados utilizando el código de validación de mensaje almacenado y la clave permanente del dispositivo pero no operable para emitir un nuevo código de validación de mensaje para los datos de restricción de utilización almacenados, y operable cuando se ha accedido de manera segura a través de la interfaz de bus, para generar un nuevo código de validación de mensaje utilizando la clave permanente y los nuevos datos de restricción de utilización cambiados que han sido generados mediante la modificación autorizada de los datos de restricción de utilización almacenados, y para emitir el nuevo código de validación de mensaje para su almacenamiento en la memoria no segura junto con los datos de restricción de utilización cambiados; un procesador de sistema (32) configurado para operar de manera selectiva en modos seguro y no seguro, y operable para un acceso no seguro al circuito criptográfico a través de la interfaz de bus para validar los datos de restricción de utilización almacenados; y operable en el modo seguro para generar los datos de restricción de utilización cambiados en respuesta a ejecutar instrucciones de programa seguras y acceder de manera segura al circuito criptográfico mediante la interfaz de bus para obtener el nuevo código de validación de mensaje para los datos de restricción de utilización cambiados; y

una memoria segura (32) para almacenar las instrucciones de programa seguras que soportan el cambio de los datos de restricción de utilización seguros, siendo la citada memoria segura accesible por el procesador del sistema en el modo seguro, caracterizada porque el circuito seguro incluye un elemento programable una sola vez (26) que indica si el dispositivo electrónico ha sido inicializado, y porque los datos de restricción de utilización almacenados comprenden una parte estática (44) y una parte dinámica (48) y los datos de restricción de utilización almacenado comprenden un primer código de validación de mensaje (46) almacenado para validar la parte estática y un segundo código de validación de mensaje (50) almacenado para validar la parte dinámica, y donde el circuito criptográfico es operable, cuando se ha accedido a él de manera segura, para generar y emitir un nuevo código de validación de mensaje para la parte estática de los datos de restricción de utilización almacenados para su almacenamiento en la memoria no segura como el primer código de validación de mensaje sólo si el elemento programable una sola vez indica que el dispositivo electrónico no ha sido inicializado.

2. El dispositivo electrónico de la reivindicación 1, en el que el procesador del sistema está configurado para iniciarse en el modo seguro en respuesta a un reinicio y a proporcionar servicio oportunamente a un temporizador de vigilante de seguridad (60) al menos en parte validando los datos de restricción de utilización almacenados y comprobándolos frente a los ajustes de Subscriber Identity Module (SIM – Módulo de Identidad de Abonado) para el dispositivo electrónico, estando el citado temporizador del vigilante de seguridad configurado para llevar a cabo un reinicio del procesador del sistema a menos que periódicamente sea servido por el procesador del sistema que opera en el modo seguro.

3. El dispositivo electrónico de la reivindicación 1, en el que el elemento programable una sola vez comprende un fusible o anti-fusible que es permanentemente alterado en respuesta a la aplicación de una señal de programa.

4. El dispositivo electrónico de la reivindicación 1, en el que el circuito seguro incluye una pluralidad de elementos programables una sola vez (28) y en el que un subconjunto de la pluralidad de elementos programables una vez están configurados para registrar la clave permanente del dispositivo como una clave (24) secreta accesible para el circuito criptográfico.

5. El dispositivo electrónico de la reivindicación 1, en el que el circuito criptográfico es operable, cuando se accede a él de manera segura, para generar el que se muestre un nuevo código de validación de mensaje para la parte dinámica de los datos de restricción de utilización almacenados para su almacenamiento en la memoria no segura como el segundo código de validación de mensaje almacenado en respuesta a órdenes seguras que le han sido proporcionadas mediante un acceso seguro por el procesador del sistema, permitiendo por ello una posterior validación de cambios autorizados llevada a cabo a la parte dinámica de los datos de restricción de utilización almacenados.

6. El dispositivo electrónico de la reivindicación 1, en el que los datos de restricción de utilización almacenados comprenden una parte estática y una parte dinámica de la información del Bloqueo del Módulo de Identidad del Abonado, y donde el circuito criptográfico está configurado para generar y emitir un primer código de validación de mensaje sólo para la parte estática como parte de la inicialización segura del dispositivo electrónico, de manera que

ningún cambio a la parte estática será validado por el circuito criptográfico, y en el que el circuito criptográfico está configurado, como parte del cambio de la parte dinámica autorizado, para generar y emitir un nuevo código de validación de mensaje para la parte dinámica, con el fin de permitir la subsiguiente validación de cambios a la parte dinámica autorizados.

7. Un método de proteger los datos de restricción de utilización que gobierna la utilización de un dispositivo electrónico, que comprende:

almacenar una clave (24) permanente del dispositivo en un circuito seguro (22)

acoplar el circuito seguro a un circuito criptográfico (18) por medio de una conexión segura (20) y

acoplar el circuito criptográfico a un procesador del sistema (32) por medio de una interfaz de bus (34),

almacenar los datos de restricción de utilización (14) como datos de restricción de utilización almacenados en una memoria (12) no segura del dispositivo electrónico, junto con un código de validación de mensaje (36) almacenado para validar los datos de restricción de utilización almacenados;

configurar el circuito criptográfico para validar (102) los datos de restricción de utilización almacenados utilizando el código de validación de mensaje almacenado y la clave permanente del dispositivo pero no generar ningún código de validación de mensaje nuevo para los datos de restricción de utilización almacenados, si se ha accedido mediante el procesador del sistema en un modo no seguro de operación;

configurar el circuito criptográfico para generar de manera selectiva (104, 158) un nuevo código de validación de mensaje utilizando la clave permanente y los datos de restricción de utilización cambiados que han sido generados mediante la modificación autorizada de los datos de restricción de utilización almacenados, y emitir (158) el nuevo código de validación de mensaje para su almacenamiento en la memoria no segura junto con los datos de restricción de utilización cambiados, si se ha accedido mediante el procesador del sistema en un modo de operación seguro;

operar en el modo seguro y en el modo no seguro basándose en que el procesador del sistema del dispositivo electrónico cambia dinámicamente entre los modos de operación seguro y no seguro, y llevando a cabo la modificación autorizada de los datos de restricción de utilización almacenados mediante la ejecución por el procesador del sistema de las instrucciones de programa seguras; y

almacenar las instrucciones de programa seguras en una memoria segura, siendo la citada memoria segura accesible por el procesador del sistema que opera en el modo seguro, caracterizado porque el método comprende también

indicar si el dispositivo electrónico ha sido inicializado mediante un elemento programable una vez incluido dentro del circuito seguro;

almacenar la clave permanente del dispositivo dentro del circuito seguro mediante una pluralidad de elementos programables una vez adicionales; y

en el que los datos de restricción de utilización almacenados comprenden una parte estática (44) y una parte dinámica (48) y el código de validación de mensaje almacenado comprende un primer código de validación de mensaje almacenado (46) para validar la parte estática y un segundo código de validación de mensaje (50) almacenado para validar la parte dinámica, y en el que la citada validación de los datos de restricción de utilización almacenados en un modo de operación no seguro comprende utilizar la clave permanente del dispositivo y los códigos de validación de mensaje almacenados primero y segundo obtenidos de la memoria no segura para validar, respectivamente, las partes estática y dinámica de la información de restricción de utilización almacenada como obtenida de la memoria no segura.

8. El método de la reivindicación 7, en el que el procesador del sistema está configurado para iniciarse en el modo seguro en respuesta a un reinicio y para servir periódicamente a un temporizador de vigilante de seguridad (60) al menos en parte validando los datos de restricción de utilización almacenados y comprobándolos frente a los ajustes del Subscriber Identity Module (SIM – Módulo de Identidad del Abonado) para el dispositivo electrónico, y comprendiendo también configurar un temporizador de vigilante de seguridad para llevar a cabo un reinicio el procesador del sistema a menos que sea oportunamente servido por el procesador del sistema que opera en el modo seguro.

9. El método de la reivindicación 7, en el que la citada generación del nuevo código de validación de mensaje en el modo de operación almacenado comprende utilizar la clave permanente del dispositivo y los datos de restricción de utilización cambiados para generar un nuevo segundo código de validación de mensaje, y emitir el nuevo segundo código de validación de mensaje para su almacenamiento como el segundo código de validación de mensaje almacenado en la memoria no segura, junto con el almacenamiento de los datos de restricción de

utilización cambiados como la parte dinámica de los datos de restricción de utilización almacenados en la memoria no segura.

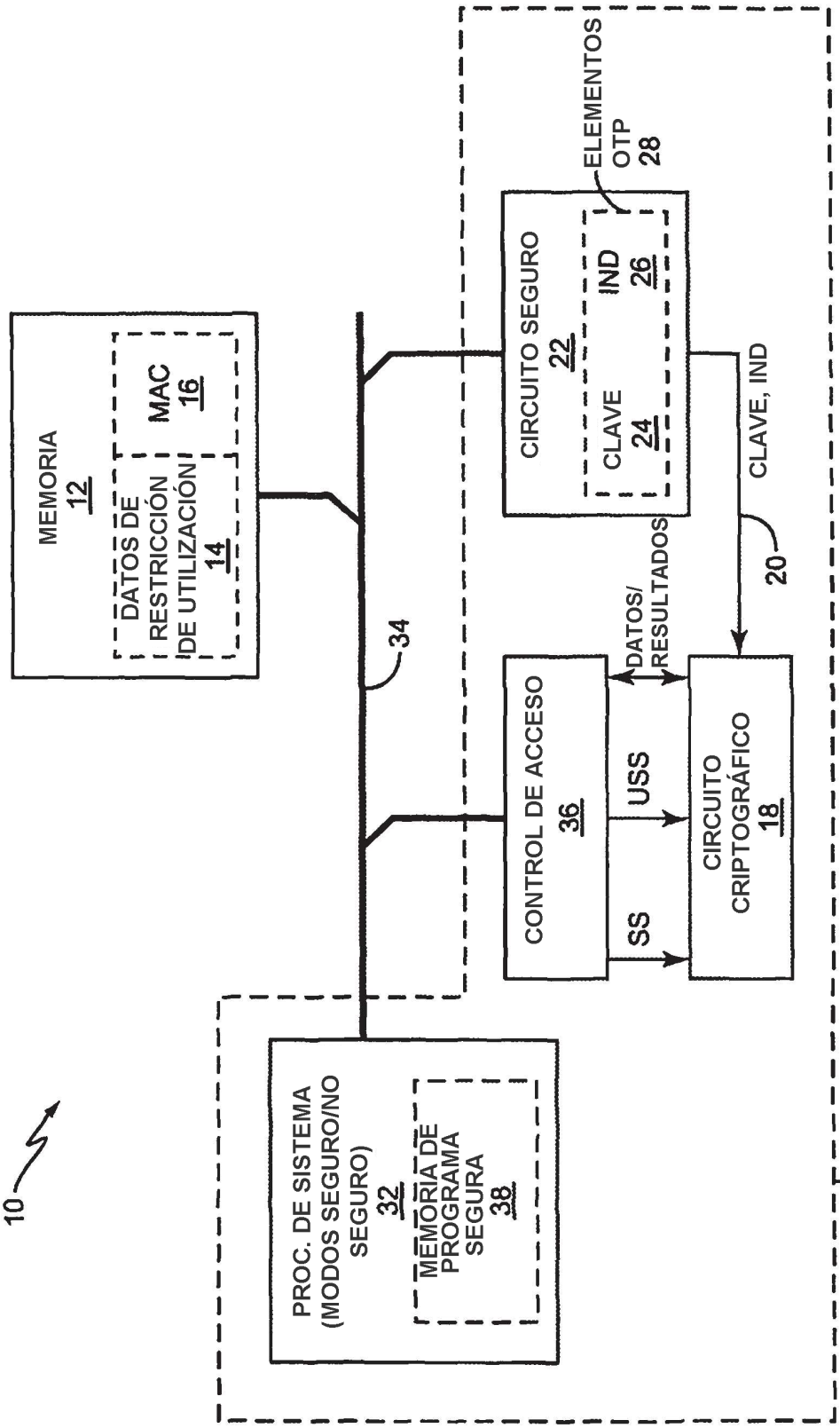
10
MEMORIA
12
DATOS DE RESTRICCIÓN DE UTILIZACIÓN
14
MAC
16
34
CIRCUITO SEGURO
22
CLAVE
24
IND
26
ELEMENTOS OTP
28
CLAVE, IND
20
DATOS/ RESULTADOS
CONTROL DE ACCESO
36
USS
SS
CIRCUITO CRIPTOGRÁFICO
18
PROC. DE SISTEMA (MODOS SEGURO/NO SEGURO)
32
MEMORIA DE PROGRAMA SEGURA
38
30

FIG. 1

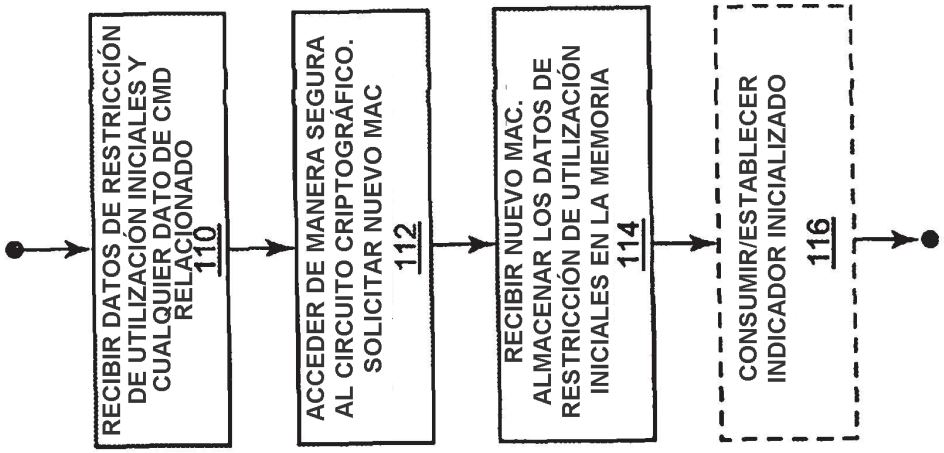

FIG. 4

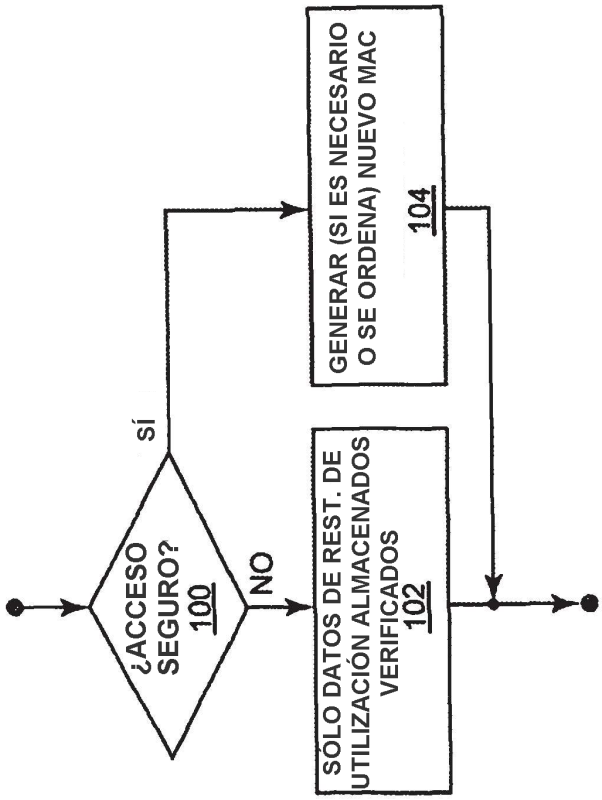

FIG. 2

FIG. 3

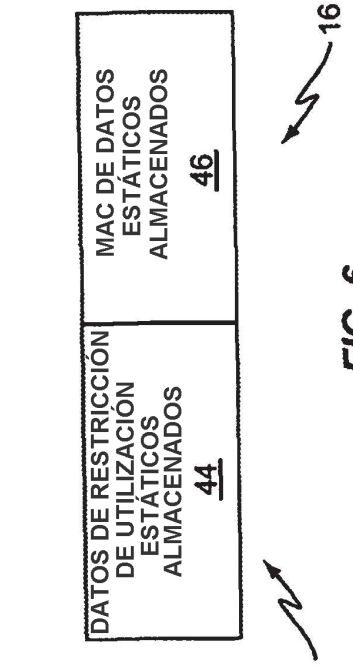
DATOS DE RESTRICCIÓN DE UTILIZACIÓN ESTÁTICOS ALMACENADOS
44
MAC DE DATOS ESTÁTICOS ALMACENADOS
46
14
16

FIG. 6

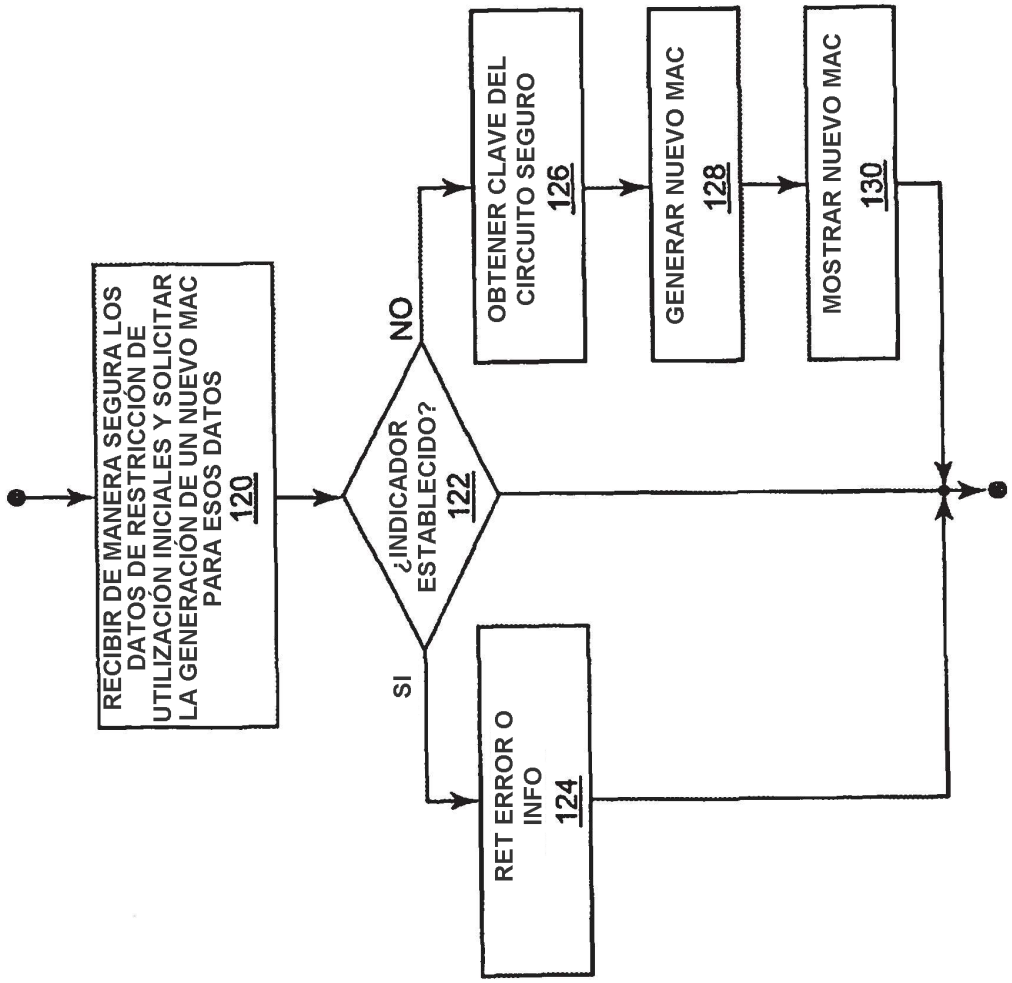
RECIBIR DE MANERA SEGURA LOS DATOS DE RESTRICCIÓN DE UTILIZACIÓN INICIALES Y SOLICITAR LA GENERACIÓN DE UN NUEVO MAC PARA ESOS DATOS
120
¿INDICADOR ESTABLECIDO?
122
NO
SI
OBTENER CLAVE DEL CIRCUITO SEGURO
126
GENERAR NUEVO MAC
128
MOSTRAR NUEVO MAC
130
RET ERROR O INFO
124

FIG. 5

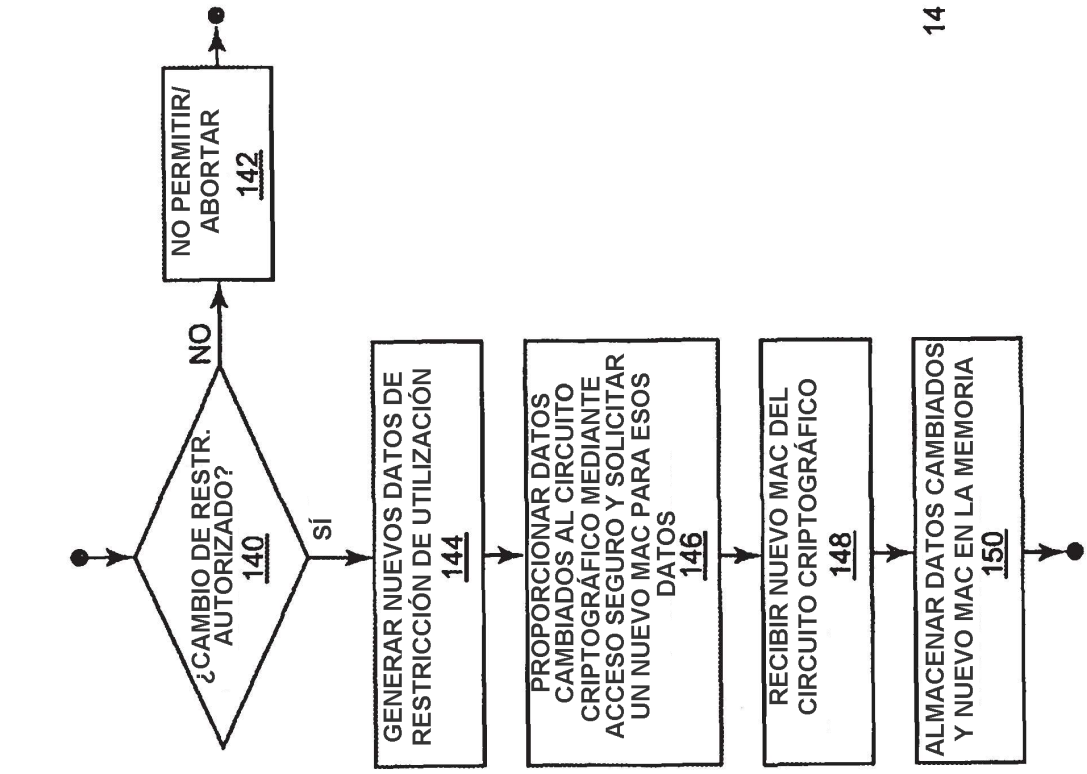

FIG. 7

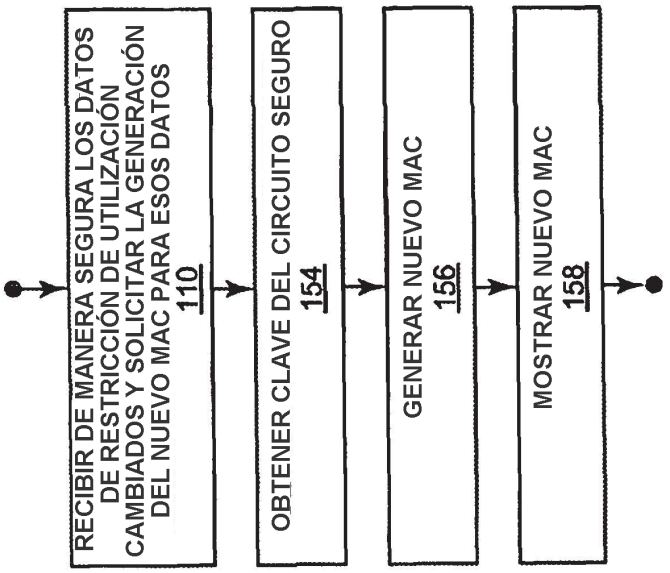

FIG. 8

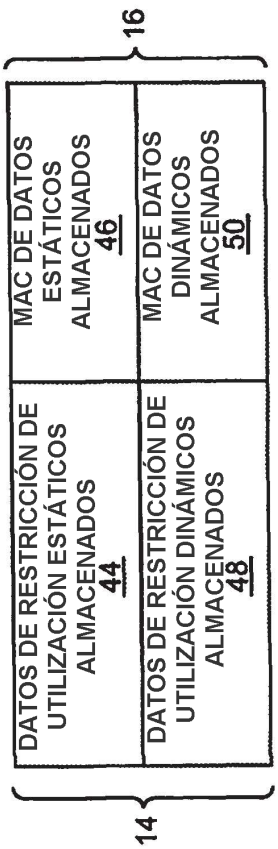

FIG. 9

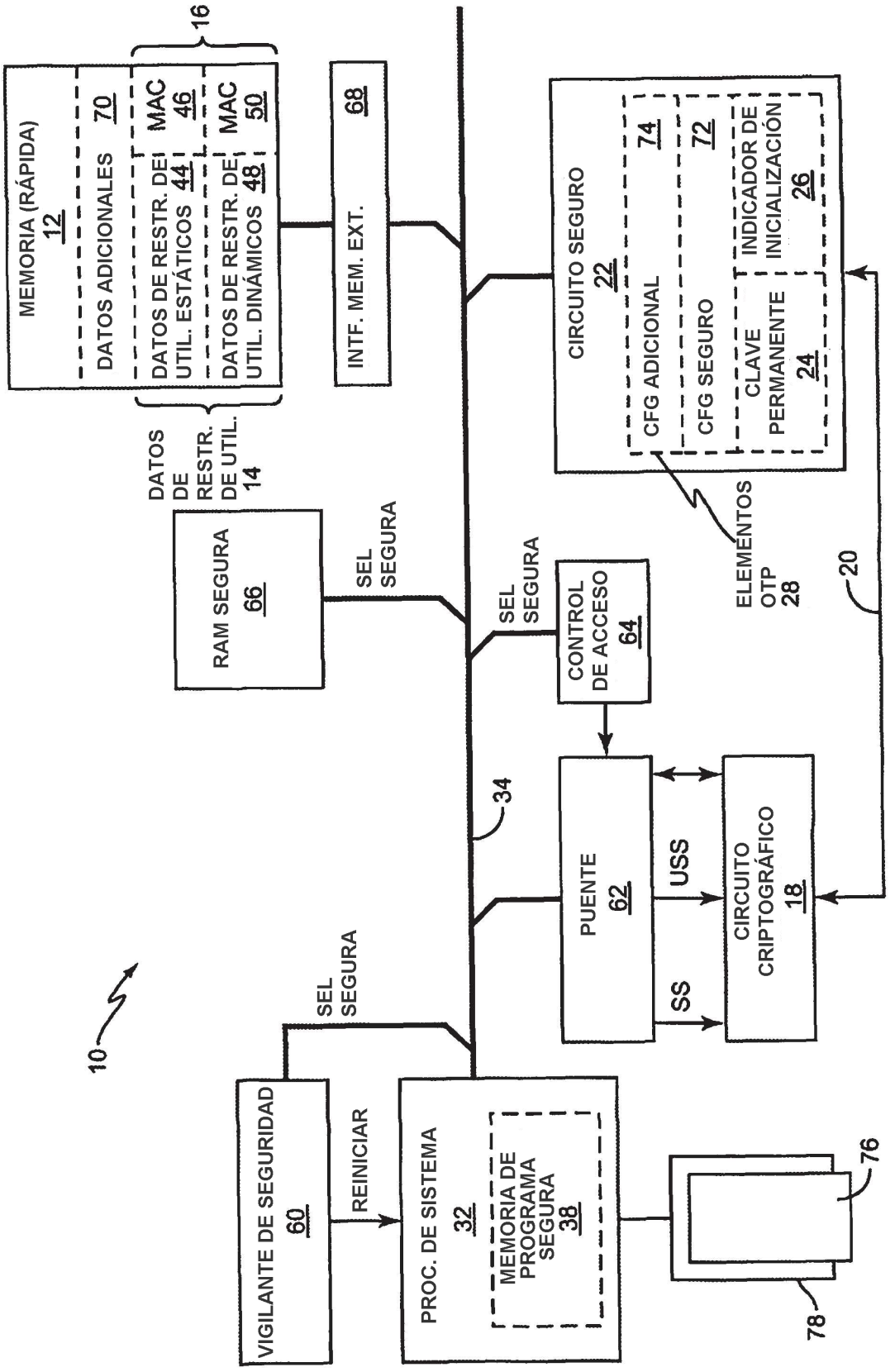
MEMORIA (RÁPIDA)
12
DATOS ADICIONALES
70
DATOS DE RESTR. DE UTIL. ESTÁTICOS
44
MAC
46
DATOS DE RESTR. DE UTIL. DINÁMICOS
48
MAC
50
16
DATOS DE RESTR. DE UTIL.
14
INTF. MEM. EXT.
68
CIRCUITO SEGURO
22
CFG ADICIONAL
74
CFG SEGURO
72
CLAVE PERMANENTE
24
INDICADOR DE INICIALIZACIÓN
26
ELEMENTOS OTP
28
20
RAM SEGURA
66
SEL SEGURA
SEL SEGURA
CONTROL DE ACCESO
64
34
PUENTE
62
USS
SS
CIRCUITO CRIPTOGRÁFICO
18
SEL SEGURA
VIGILANTE DE SEGURIDAD
60
REINICIAR
PROC. DE SISTEMA
32
MEMORIA DE PROGRAMA SEGURA
38
76
78
10

FIG. 10