(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 357 421**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **02755462 .5**
(96) Fecha de presentación : **13.08.2002**
(97) Número de publicación de la solicitud: **1535124**
(97) Fecha de publicación de la solicitud: **01.06.2005**

(54) Título: **Arquitectura informática para ejecutar un programa en un modo seguro o no seguro.**

(45) Fecha de publicación de la mención BOPI:
26.04.2011

(45) Fecha de la publicación del folleto de la patente:
26.04.2011

(73) Titular/es: **NOKIA CORPORATION**
Keilalahdentie 4
02150 Espoo, FI

(72) Inventor/es: **Paatero, Lauri y**
Kiiveri, Antti

(74) Agente: **López Bravo, Joaquín Ramón**

DESCRIPCIÓN

Campo técnico de la invención

La presente invención se refiere a una circuitería para proporcionar seguridad de datos, dicha circuitería contiene al menos un procesador y al menos un circuito de almacenamiento. La presente invención se refiere también a un procedimiento para proporcionar seguridad de datos en una circuitería que contiene al menos un procesador y al menos un circuito de almacenamiento.

Técnica anterior

Varios dispositivos electrónicos, tales como terminales móviles de telecomunicación, ordenadores portátiles y PDA requieren acceso a componentes relacionados con la seguridad, tales como programas de aplicación, claves criptográficas, material de datos de claves criptográficas, resultados intermedios de cálculos criptográficos, contraseñas, autenticación de datos externamente descargados, etc. A menudo es necesario que estos componentes, y el procesamiento de los mismos, se mantenga secreto dentro del dispositivo electrónicamente, Idealmente, serán conocidos por las menos personas posibles. Esto es debido al hecho de que un dispositivo, por ejemplo un terminal móvil, podría posiblemente ser manipulado, si se conociesen estos componentes. El acceso a este tipo de componentes puede ayudar a un malhechor con malas intenciones a manipular un terminal.

Asimismo, en los dispositivos, los componentes relacionados con la seguridad, anteriormente mencionados serán manejados, procesados y administrados junto a componentes más generales que no requieren ningún procesamiento seguro. Por lo tanto, se introduce un entorno de ejecución seguro, en cuyo entono un procesador en el interior del dispositivo electrónico es capaz de acceder a los componentes relacionados con la seguridad. El acceso al entorno de ejecución seguro, el procesamiento en el y la salida del mismo se deberían controlar cuidadosamente. El hardware de la técnica anterior que comprende este entorno seguro está a menudo confinado dentro de un paquete resistente a la manipulación. No debería ser posible explorar o llevar a cabo mediciones y ensayos en este tipo de hardware que pudiesen dar como resultado la revelación de los componentes relacionados con la seguridad y el procesamiento de los mismos.

Un dispositivo electrónico que procesa información en un entorno seguro y que almacena información relacionada con la seguridad de una manera segura se muestra en la patente de los Estados Unidos nº 5.892.900. La patente divulga un entorno de distribución virtual que protege, administra y controla el uso de información electrónica. Comprende una solución de protección de derechos para los distribuidores, proveedores de servicios financieros, usuarios finales y otros. La invención usa dispositivos electrónicos denominados Unidades de Procesamiento Seguros para proporcionar seguridad y almacenamiento y comunicación seguros de información. Tal dispositivo, que incluye un procesador, está confinado dentro de una “barrera de seguridad resistente a la manipulación”, que separa el entorno seguro del mundo exterior. El dispositivo electrónico proporciona tanto el entorno seguro como un entorno no seguro, en este último caso el procesador del dispositivo no tiene acceso a la información relacionada con la seguridad

Un problema que ha de ser resuelto, es permitir que una tercera parte lleve a cabo el ensayo, la depuración y el mantenimiento del dispositivo electrónico y su software sin correr el riesgo de que esta tercera parte acceda a la información que hace posible manipular los componentes relacionados con la seguridad del dispositivo llegando a afectar a las funciones de seguridad cuando se encuentra en entorno seguro. Debería ser posible moverse entre los dos entornos suavemente, sin tener que reiniciar el uno o el otro cada vez que se efectúa un movimiento.

El documento EP-A-1262856 representa un documento de la técnica anterior según el artículo 54(3) CEP. El documento US-A-57537760 divulga un microcontrolador que trabaja en un modo seguro o un modo no seguro indicado por un registro de control. El microcontrolador proporciona seguridad a las instrucciones internas y los datos almacenados en una memoria ROM a la vez que permite que una instrucción acceda a una memoria externa fuera de chip conectada a un bus de expansión. Si se lleva a cabo el acceso a la ROM, la lógica de seguridad se pone en un primer modo operativo denominado modo no seguro en el cual la circuitería de seguridad permite el acceso de las instrucciones a ambas memorias. Una vez que la CPU del microcontrolador lleva a cabo un acceso a una instrucción fuera de chip (por el bus de expansión), la lógica de seguridad se pone en un modo seguro en el cual el acceso a la ROM no es permitido por un usuario que tiene acceso a la ROM por el bus de expansión.

Sumario de la invención

Un objeto de la presente invención es proporcionar una solución al problema dado anteriormente proponiendo una arquitectura que comprende un entorno seguro en el cual es posible almacenar y procesar información, tal como claves criptográficas y otros datos relacionados con la seguridad, de una manera segura y siendo posible ademas ensayar y depurar la arquitectura y su software acompañante en un entorno seguro sin proporcionar acceso a los datos de seguridad.

Este objeto se consigue mediante la invención en un primer aspecto en forma de circuitería para proporcionar seguridad de datos, dicha circuitería contiene al menos un procesador y al menos un circuito de almacenamiento según la reivindicación 1 y en un segundo aspecto en forma de un procedimiento para proporcionar seguridad de datos en una circuitería que contiene al menos un procesador y al menos un circuito de almacenamiento según la reivindicación 6. Las realizaciones preferidas están definidas por las reivindicaciones dependientes.

Un primer aspecto de la invención se refiere a por la circuitería que comprende al menos un área de almacenamiento en un circuito de almacenamiento, en la cual se sitúan los datos protegidos del área de almacenamiento relativos a la seguridad de la circuitería. La circuitería está dispuesta con medios de ajuste de modo dispuestos para instalar un procesador comprendido en la circuitería en uno de al menos dos modos operativos diferentes, siendo los medios de ajuste de modo capaces de alterar los modos operativos del procesador. Asimismo, comprende medios de control de acceso al circuito de almacenamiento dispuestos para controlar que el procesador accede al área de almacenamiento en la cual se encuentran los datos protegidos basados en un primer modo operativo, y dispuestos para evitar que el procesador acceda al área de almacenamiento en la cual se encuentran los datos protegidos, basados en un segundo modo operativo del procesador, permitiendo de este modo que el procesador ejecute software no verificado descargado en la circuitería.

Un segundo aspecto de la invención se refiere a, un procedimiento en el cual los datos protegido relativos a la seguridad de la circuitería se almacenan en un circuito de almacenamiento. Un procesador se ajusta en uno de al menos dos diferentes modos operativos alterables. El procedimiento comprende, además, la etapa de permitir que el procesador acceda a un área en la cual se encuentran los datos protegidos poniendo el procesador en un primer modo operativo y evitando que el procesador acceda al área de almacenamiento en la cual se encuentran los datos protegidos poniendo el procesador en un segundo modo operativo, permitiendo de este modo que el procesador ejecute software no verificado descargado en la circuitería.

La invención se basa en la idea de que se proporciona una circuitería en la cual puede funcionar un procesador en al menos dos modos diferentes, un primer modo operativo seguro y un segundo modo operativo no seguro. En el modo seguro, el procesador tiene acceso a los datos relacionados con la seguridad que se encuentran en varias memorias situadas dentro de la circuitería. Los datos de seguridad incluyen claves criptográficas y algoritmos, software para poner en marcha la circuitería, datos secretos tales como números aleatorios usados como material de calves criptográficas, programas de aplicación, etc. La circuitería se puede usar ventajosamente en terminales móviles de telecomunicaciones pero también en otros dispositivos electrónicos, tales como ordenadores, PDA u otros dispositivos con necesidades de protección de datos. En el caso en que la circuitería se encuentra dentro de un terminal móvil de telecomunicación, debería ser deseable que la circuitería proporcione al terminal un único número de identificación y claves acompañantes para operaciones criptográficas en el número de identificación. El acceso a estos datos de seguridad y el procesamiento de los mismos necesita ser limitado, ya que un intruso con acceso a los datos de seguridad podría manipular el terminal. Cuando se ensaya y/o depura el Terminal, el acceso a la información de seguridad no está permitido. Por esta razón, el procesador se pone en el modo operativo no seguro, en cuyo modo ya no se proporciona acceso a los datos protegidos.

La invención permite ventajosamente que el procesador de la circuitería ejecute software no verificado descargado dentro de la circuitería. Esto permite ensayar, depurar y mantener el dispositivo electrónico y su software sin correr el riesgo de que una tercera parte tenga acceso a la información que hace posible manipular los componentes relacionados con la seguridad afectando de este modo las funciones de seguridad cuando se encuentra en el entorno seguro.

Se ha de observar que en la patente de los Estados Unidos nº 5.892.900, el modo no seguro es el modo “normal”, usado cuando las transacciones y comunicaciones deben ser seguras, mientras que en la presente invención, el modo seguro es el modo normal. En la presente invención, el modo no seguro se introduce solamente durante el ensayo y/o la depuración u otros tipos de casos especiales cuando se deben proteger los datos de

seguridad, es decir, cuando el modo seguro no puede prácticamente mantenerse.

La presente invención elimina el uso de terminales de fines especiales adaptados para su uso en investigación y desarrollo. Durante una etapa de desarrollo, a veces una condición es poder descargar un código no fiable y/o no verificado en los terminales. Permitiendo el modo inseguro, se proporciona un canal dentro del terminal sin dar acceso a los componentes relacionados con la seguridad. En consecuencia, el mismo terminal se puede utilizar para una operación normal así como en la etapa de desarrollo. Se ha de entender que es más caro fabricar terminales de fines especiales.

Según una realización de la invención, la circuitería de la invención se dispone con un temporizador que controla el periodo de tiempo durante el cual el procesador está en modo no seguro. Si fallasen otras acciones de control de seguridad, se establece un periodo máximo de tiempo dado durante el cual se da acceso a un modo no seguro del procesador. Esto limita la posibilidad de que un intruso realice la depuración y el ensayo del dispositivo.

Según la invención se proporcionan medio de autenticación, estando dichos medios dispuestos para autenticar datos proporcionados externamente al terminal. Una ventaja con esta característica es que durante la etapa de fabricación, y otras etapas conde el modo operativo seguro normal ya no está activado, el terminal se puede usar durante un periodo de tiempo limitado, suficiente para cargar un código firmado aceptado en el terminal. También es posible descargar paquetes de códigos firmados dentro del terminal durante la operación en modo seguro. Esto facilita la posibilidad de añadir nuevas características de seguridad al terminal proporcionando flexibilidad a la arquitectura. La arquitectura permite que las aplicaciones se dividan en partes seguras y no seguras. El circuito verifica los paquetes de códigos que están adecuadamente firmados. Las aplicaciones seguras se descargan a, y se ejecutan desde, el área de almacenamiento que contienen los datos protegidos. Esto hace que la descarga de los datos sea más suave. Si esta características no estuviese presente, sería necesario descargar aplicaciones seguras y aplicaciones no seguras por separado.

Según otra realización más de la invención, la circuitería está dispuesta con medios para la indicación del modo en el cual está funcionando el procesador. Es apropiado que se establezca un registro de modos dentro de la circuitería, mantener un control de modo actual. En el caso de que la circuitería esté dispuesta dentro de un terminal móvil de comunicación, sería posible indicar en la pantalla del terminal, por el altavoz del terminal o por cualquier otro modo, al usuario del terminal el hecho de que el terminal está funcionando en modo no seguro. Esto avisara al usuario sobre el hecho de que se ha introducido el modo no seguro.

Según otras realizaciones de la presente invención, los medios de establecimiento de modo dispuestos para controlar los modos del procesador comprenden un programa de aplicación. Esto tiene la ventaja de que el modo se podría ajustar por el propio dispositivo, sin tener que depender de señales externas. Desde el punto de vista de la seguridad, se prefiere esto último ya que controlando el software de aplicación, se puede controlar también el establecimiento de los modos de procesador. También es posible tener una señal externa conectada a la circuitería, mediante cuya señal es posible controlar el modo del procesador. Usando una señal externa, se puede ejecutar un cambio de modo fácil y rápidamente, lo cual puede ser ventajoso en entornos de ensayo. Una combinación de estos dos medios de ajuste de modos es factible.

Breve descripción de los dibujos

La presente invención se describirá en mayor detalle con referencia a los siguientes dibujos, en el cual:

La figura 1 muestra un diagrama de bloques de una realización preferida de circuitería para proporcionar seguridad de datos según la presente invención; y

La figura 2 muestra un diagrama de flujo de procedimiento de arranque para la circuitería según la presente invención.

Descripción de realizaciones preferidas de la invención

La figura 1 muestra un diagrama de bloques de una realización preferida de la presente invención. Como se puede ver, la arquitectura en la figura 1 contiene tanto software como hardware. La arquitectura se implementa en forma de un ASIC (Circuito integrado específico de aplicación). La parte de procesamiento de la arquitectura contiene una CPU y un procesador de señal digital DSP. Estos dos procsadores se pueden fusionar en un solo procesador. Normalmente la CPU se ocupa de las operaciones de comunicación y el DSP se ocupa del cálculo de datos.

El entorno seguro comprende una memoria ROM a partir de la cual se pone en marcha el ASIC. Esta memoria ROM contiene software de aplicación de arranque y un sistema operativo OS. El sistema operativo controla y ejecuta aplicaciones y ofrece varios servicios de seguridad a las aplicaciones tales como control de la integridad del software de aplicación y control de acceso. El sistema operativo tiene acceso al hardware de ASIC y no puede proporcionar el mismo seguridad rigurosa de hardware, pero puede contar con la arquitectura de seguridad.

Algunos programas de aplicación que residen en el entorno seguro, es decir, el área de almacenamiento de datos protegidos, tiene prioridad sobre otros programas de aplicación. En un terminal móvil de comunicación, en el cual se puede disponer el ASIC, debería existir un software de arranque, dicho software incluye la funcionalidad principal del terminal. No es posible poner en marcha el terminal en modo operativo normal sin este software. Esto tiene la ventaja de que controlando este software de puesta en marcha, también es posible controlar la activación inicial de cada terminal.

El entorno seguro comprende, también memoria RAM para el almacenamiento de datos y aplicaciones. La memoria RAM almacena preferiblemente aplicaciones denominadas protegidas, que son aplicaciones de menor tamaño para llevar a cabo operaciones críticas de seguridad en el interior del entorno seguro. Normalmente, la manera de utilizar las aplicaciones protegidas es dejar que las aplicaciones “normales” soliciten servicios de alguna aplicación protegida. Las nuevas aplicaciones protegidas se pueden descargar en el entorno seguro en cualquier momento, lo cual no sería el caso si residiesen en la memoria ROM. El software de entorno seguro controla la descarga y ejecución de aplicaciones protegidas. Solamente se permiten que funcionen las aplicaciones protegidas firmadas. Las aplicaciones protegidas pueden acceder a cualesquiera recursos en el entorno seguro y pueden también comunicar con aplicaciones normales para la prestación de servicios de seguridad.

En el entorno seguro, se cuenta con una memoria fusible que contiene un solo número aleatorio que se genera y programa en el ASIC durante la fabricación. Este número aleatorio se usa como la identidad de un ASIC específico y se emplea, además, para derivar claves para operaciones criptográficas. Asimismo, se disponen medios de control de acceso al circuito de almacenamiento en forma de un registro de control de seguridad. El fin del registro de control de seguridad es proporcionar el acceso de CPU al entorno seguro, dependiendo del modo establecido en el registro. Los modos operativos del procesador se pueden establecer en el registro por el software de aplicación, dando como resultado el hecho de que la arquitectura no tiene que contar con señales externas. Desde un punto de vista de la seguridad, esto es preferible ya que controlando el software de aplicación, el ajuste de los modos del procesador también se puede controlar. Es también posible tener una señal externa (no mostrada) conectada al ASIC, mediante cuya señal es posible establecer el registro de control de seguridad. Usando una señal externa, se puede ejecutar un cambio de modo fácil y rápidamente, que puede ser ventajoso en entornos de ensayos. Una combinación de estos dos medios de ajuste de modo es factible.

Preferiblemente, el terminal móvil de telecomunicaciones debería indicar en la pantalla del terminal, mediante el altavoz del terminal o de cualquier otra manera visual, a un usuario del terminal el hecho de que el terminal está funcionando en modo no seguro. Esto avisará al usuario sobre el hecho de que se ha introducido el modo no seguro.

Se dispone una función de vigilancia para varios fines de temporización. En caso de que la verificación de firma del software descargado falle, las sumas de comprobación no coinciden o se detecta algún otro error, la operación del ASIC o el terminal móvil de telecomunicación en el que está dispuesta debería pararse. Esto preferiblemente no se debería hacer inmediatamente cuando ocurre el error. Se desea un tiempo límite aleatorio, por ejemplo, un tiempo diferente que se extiende a lo largo de hasta 30 segundos. Esto hace más difícil el hecho de que un malhechor detecte el instante en el cual el terminal ha detectado el error. La inhabilitación de la actualización de la función de vigilancia se establece en el registro de control de seguridad. El resultado de esta operación es que el propio terminal se reiniciará. La función de vigilancia también puede controlar el periodo de tiempo durante el cual el procesador está en el modo no seguro. Si fallasen otras acciones de control de seguridad, se establece un periodo de tiempo máximo dado durante el cual se da acceso al modo no seguro del procesador. Esto limita la posibilidad de que un intruso lleve a cabo la depuración y el ensayo del dispositivo.

La CPU se conecta al hardware de entorno seguro mediante una unidad de gestión de memoria MMU que se ocupa de las operaciones de memoria. También cartografía direcciones virtuales en direcciones físicas en la memoria para los procesos ejecutados en la CPU. La MMU se sitúa en un bus que contiene señales de datos, direcciones y de control. También es posible tener una segunda MMU dispuesta para ocuparse de las operaciones de memoria para la memoria RAM de ASIC situada fuera del entorno seguro. Un circuito de punte estándar para la limitación de la visibilidad de los datos sobre el bus se dispone dentro del ASIC. La arquitectura se debería confinar

dentro de una envoltura resistente a la manipulación. No debería ser posible explorar o llevar a cabo mediciones y ensayos sobre este tipo de hardware que pudiesen dar como resultado la revelación de componentes relacionados con la seguridad y el procesamiento de los mismos. El DSP tiene acceso a otros periféricos tales como una unidad de acceso directo de memoria (DMA) La DMA es proporcionada por la arquitectura para permitir que los datos sean enviados directamente desde el DSP a una memoria. El DSP se libera de la relación con la transferencia de datos, acelerando de este modo la operación global. Otros periféricos tales como memorias RAM, rápidas y procesadores adicionales se pueden disponer fuera del ASIC. Una memoria RAM se dispone también fuera del entorno seguro en el ASIC, guardando dicha RAM el software no verificado ejecutado por la CPU.

Proporcionando la arquitectura anteriormente descrita en la cual la CPU se puede utilizar en dos modos diferentes, un modo operativo seguro y un modo operativo no seguro, la CPU de la arquitectura se puede habilitar para ejecutar software no verificado descargado en el ASIC. Esto es debido al hecho de que solamente el software verificado tiene acceso al entorno seguro. Esto permite ensayar, depurar y mantener el terminal móvil de telecomunicación y su software sin correr el riesgo de que una tercera persona tenga acceso a la información que hiciese posible que manipulase los componentes relacionados con la seguridad del dispositivo afectando de este modo a las funciones de seguridad cuando se encuentran en el entorno seguro.

En el modo seguro, el procesador tiene acceso a datos relacionados con la seguridad situados en e entorno seguro. Los datos de seguridad incluyen claves criptográficas y algoritmos, software para poner en marcha la circuitería, datos secretos tales como números aleatorios usados como material de claves criptográficas, programas de aplicación, etc. La circuitería se puede usar ventajosamente en terminales móviles de telecomunicaciones pero también en otros dispositivos electrónicos tales como ordenadores, PDA u otros dispositivos con necesidades de protección de datos. El acceso a estos datos de seguridad y el procesamiento de los mismos necesitan ser limitados, ya que un intruso con acceso a los datos de seguridad podría manipular el terminal. Cuando se ensaya y/o depura el terminal el acceso a la información de seguridad no está permitido. Por esta razón, el procesador se pone en el modo operativo no seguro, en cuyo modo ya no se proporciona acceso a los datos protegidos dentro del entorno seguro.

La figura 2 ilustra un diagrama de flujo del proceso de puesta en marcha bajo tensión para la arquitectura. En la puesta bajo tensión, el software de arranque de ROM activa el modo seguro para la configuración inicial. A continuación se verifican las firmas para la primera aplicación protegida y el sistema operativo a descargar. Si las firmas son correctas, la aplicación y el sistema operativo se descargan en la RAM de entorno seguro. Cuando el software deseado se ha descargado, se informa a la CPU de que la descarga se ha terminado y la CPU empieza a ejecutar el software verificado. El sistema operativo y la aplicación protegida se han descargado de este modo en el entorno seguro de una manera segura y fiable.

Sin embargo, si la verificación de firmas falla o si la firma no está presente, se activa el modo no seguro y la operación no verificada se carga en la RMA del ASIC situada fuera del entorno seguro. Posiblemente, la función de vigilancia se establece para limitar el periodo de tiempo durante el cual está activado el modo no seguro. Se establece un periodo de tiempo máximo durante el cual está activo el modo no seguro. Cuando se completa la puesta en marcha, esta aplicación no verificada es ejecutada por la CPU. El entorno seguro es ahora inaccesible.

Aunque la invención se ha descrito con referencia a realizaciones ejemplares específicas de la misma, muchas alteraciones, modificaciones y similares diferentes serán evidentes para el experto en la técnica. Las realizaciones descritas no pretenden, por lo tanto, limitar el alcance de la invención, definido por las reivindicaciones anexas.

REIVINDICACIONES

1.- Circuitería para proporcionar seguridad de datos, dicha circuitería contiene al menos un procesador y al menos un circuito de almacenamiento y dicha circuitería comprende:

Al menos un área de almacenamiento en dicho circuito de almacenamiento, en la cual área de almacenamiento se sitúan los datos protegidos relativos a la seguridad de la circuitería;

medios de ajuste de modo dispuestos para ajustar medios de control de acceso del circuito de almacenamiento para indicar uno al menos de dos modos operativos diferentes, siendo los medios de ajuste de modo capaces de alterar los modos operativos del procesador;

Dichos medios de control de acceso del circuito de almacenamiento dispuestos para controlar que el procesador para que opere en un primer modo operativo o un segundo modo operativo del procesador de dichos al menos dos modos operativos diferentes,

El primer modo operativo permite que dicho procesador acceda a dicha área de almacenamiento en la cual se encuentran dichos datos protegidos y el segundo modo operativo evita que el procesador acceda a dicha área de almacenamiento en la cual se encuentran los datos protegido, en la cual dicho procesador gestiona todos los accesos a dicha área de almacenamiento para proteger dichos datos protegidos situados en dicha área de almacenamiento,

caracterizada porque

medios de autenticación dispuestos, en la puesta bajo tensión, para autenticar, por verificación de firma, un software no verificado descargado en la circuitería en dicho primer modo operativo;

en la que dicho modo operativo de procesador se ajusta en dicho segundo modo operativo de procesador cuando un software no verificado a descargar no se ha autenticado en dichos medios de autenticación

permitiendo de este modo que dicho al menos un procesador ejecute software no verificado descargado en la circuitería.

2.- Circuitería para proporcionar seguridad de datos según la reivindicación 1, que comprende, además:

un temporizador dispuesto para controlar el periodo de tiempo durante el cual el procesador está en dicho modo operativo no seguro.

3.- Circuitería para proporcionar seguridad de datos según cualquiera de las reivindicaciones anteriores, que comprende, además:

medios dispuestos para indicar en qué modo está operando el procesador.

4.- Circuitería para proporcionar seguridad de datos según cualquiera de las reivindicaciones anteriores, en la cual dichos medios de ajuste de modo comprenden un programa de aplicación.

5.- Circuitería para proporcionar seguridad de datos según cualquiera de las reivindicaciones anteriores, dicha circuitería está comprendida en un terminal móvil de telecomunicación.

6.- Procedimiento para proporcionar seguridad de datos en una circuitería que contiene al menos un procesador y al menos un circuito de almacenamiento y dicho procedimiento comprende las etapas de:

almacenar datos protegidos relacionados con la seguridad de la circuitería en al menos un área de almacenamiento en dicho circuito de almacenamiento

ajustar medios de control de acceso al circuito de almacenamiento para indicar uno de al menos dos modos operativos de procesador diferentes, siendo capaz el medio de ajuste de modificar el modo operativo de procesador del procesador;

controlar mediante dichos medios de control de acceso al circuito de almacenamiento el procesador para que opere en un primer modo operativo de procesador o un segundo modo operativo del procesador de dichos al menos dos modos operativos diferentes,

en el cual el primer modo operativo permite que dicho procesador acceda a dicha área de almacenamiento en la cual se encuentran dichos datos protegidos y el segundo modo operativo evita que el procesador acceda a dicha área de almacenamiento en la cual se encuentran los datos protegido, y en el que dicho procesador gestiona todos los accesos a dicha área de almacenamiento para proteger dichos datos protegidos situados en dicha área de almacenamiento,

caracterizado por las etapas de:

en la puesta bajo tensión, autenticar, por verificación de firma, un software no verificado descargado en la circuitería en dicho primer modo operativo;

ajustar dicho modo operativo de procesador en dicho segundo modo operativo de procesador cuando un software no verificado a descargar no se ha autenticado en dicha etapa autenticación,

permitir de este modo que dicho al menos un procesador ejecute software no verificado descargado en la circuitería.

7.- Procedimiento para proporcionar seguridad de datos según la reivindicación 6, que comprende, además, la etapa de:

controlar el periodo de tiempo durante el cual el procesador está en dicho modo operativo no seguro mediante un temporizador.

8.- Procedimiento para proporcionar seguridad de datos según cualquiera de las reivindicaciones 6-7, que comprende, además, la etapa de:

indicar en qué modo está operando el procesador.

9.- Procedimiento para proporcionar seguridad de datos según cualquiera de las reivindicaciones 6-8, en la cual el ajuste de dicho procesador en uno de al menos dos modos operativos alterables diferentes se lleva a cabo mediante un programa de aplicación.

10.- Procedimiento para proporcionar seguridad de datos según cualquiera de las reivindicaciones 6-9, en el cual la circuitería que contiene al menos un procesador y al menos un circuito de almacenamiento está dispuesta en un terminal móvil de telecomunicación.

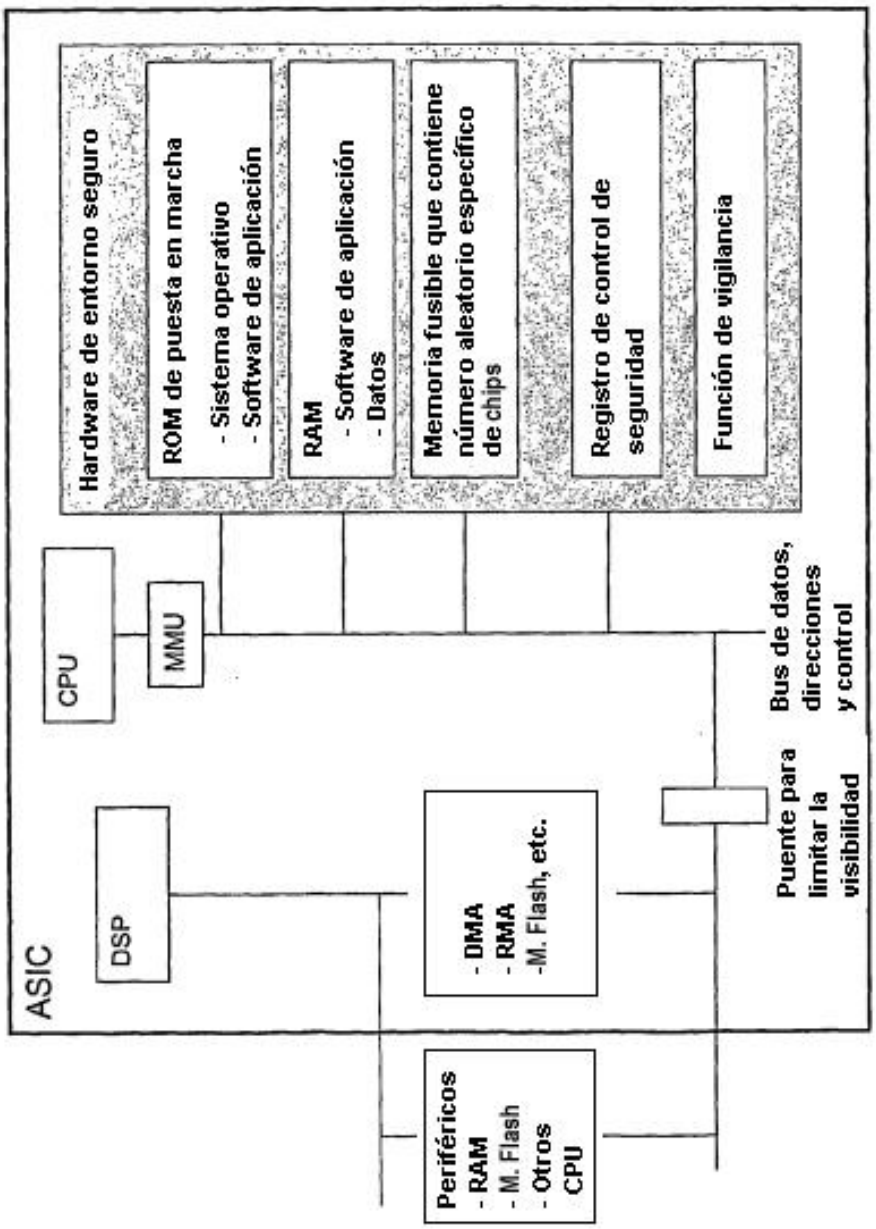
ASIC
CPU
MMU
DSP
Hardware de entorno seguro
ROM de puesta en marcha
- Sistema operativo
- Software de aplicación
RAM
- Software de aplicación
- Datos
Memoria fusible que contiene número aleatorio específico de chips
Registro de control de seguridad
Función de vigilancia
- DMA
- RMA
-M. Flash, etc.
Puente para limitar la visibilidad
Bus de datos, direcciones y control
Periféricos
- RAM
- M. Flash
- Otros CPU

Fig. 1

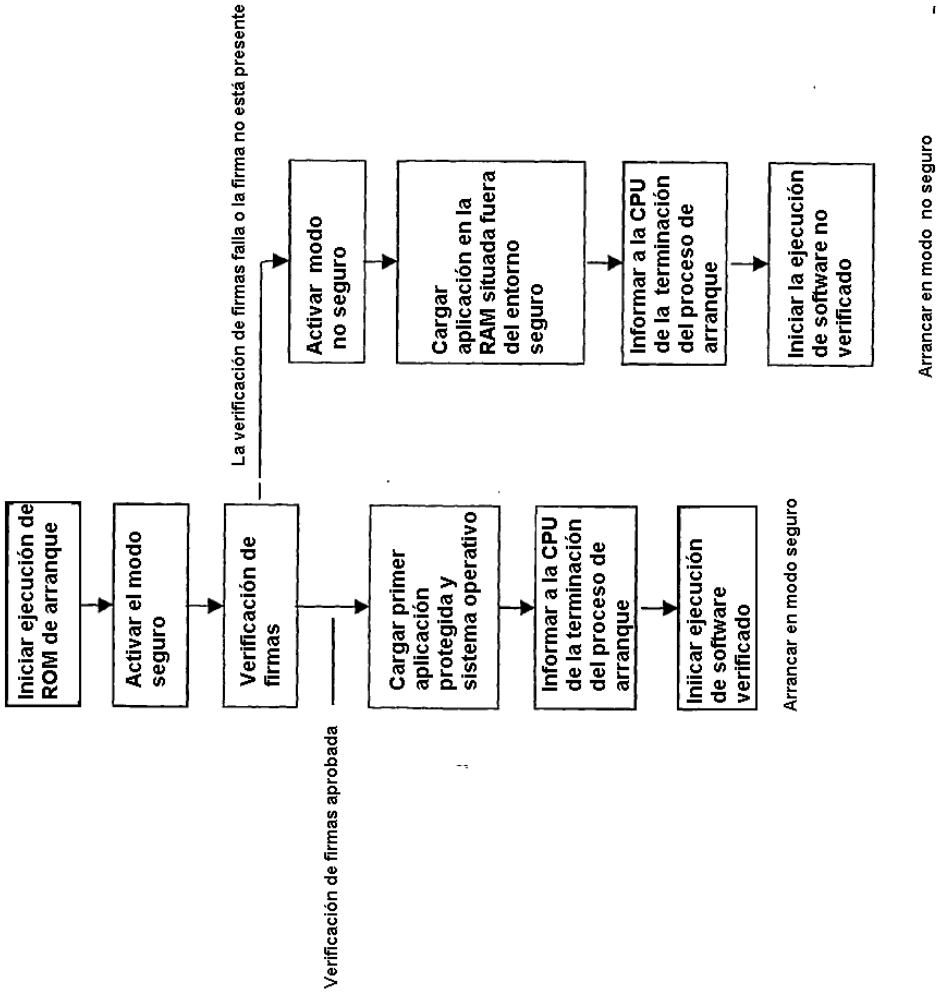
Iniciar ejecución de ROM de arranque
Activar el modo seguro
Verificación de firmas
La verificación de firmas falla o la firma no está presente
Activar modo no seguro
Cargar aplicación en la RAM situada fuera del entorno seguro
Informar a la CPU de la terminación del proceso de arranque
Iniciar la ejecución de software no verificado
Arrancar en modo no seguro
Verificación de firmas aprobada
Cargar primer aplicación protegida y sistema operativo
Informar a la CPU de la terminación del proceso de arranque
Iniicar ejecución de software verificado
Arrancar en modo seguro

Fig. 2