(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 397 628**

(51) Int. CI.:

H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **26.02.2003 E 03702946 (9)**

(97) Fecha y número de publicación de la concesión europea: **19.12.2012 EP 1479187**

(54) Título: **Control de niveles de acceso en teléfonos por certificados**

(30) Prioridad:

28.02.2002 US 90426

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.03.2013

(73) Titular/es:

NOKIA CORPORATION (100.0%)
Keilalahdentie 4
02150 Espoo, FI

(72) Inventor/es:

PAATERO, LAURI

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Control de niveles de acceso en teléfonos por certificados

Campo técnico:

La presente invención se dirige al control de la funcionalidad de niveles de seguridad en dispositivos y en particular, al control de la funcionalidad crítica de la seguridad en dispositivos inalámbricos.

Antecedentes de la invención:

Los dispositivos inalámbricos y en particular los teléfonos móviles tienen un número en aumento de funciones críticas de seguridad incorporadas en los dispositivos. Tales funciones incluyen la capacidad de firmar los datos, para presentar el contenido protegido usando la gestión de derechos digitales (DRM) y actividades similares. Algunas de estas características se están diseñando actualmente en los teléfonos inalámbricos.

Se contempla que en el futuro cada teléfono móvil tendrá una identidad permanente incorporada dentro del teléfono. Tal identidad se puede usar para impedir una modificación de la Identidad del Equipo de estación Móvil Internacional (IMEI) comúnmente usada con los teléfonos móviles. Los teléfonos móviles también tendrán una clave privada secreta para su uso en las infraestructuras de claves públicas (PKI). Además, se usará la firma del código en los teléfonos móviles para controlar la ejecución o la instalación de código de ordenador relacionado con la seguridad. La mayor parte de los códigos de ordenador críticos para la seguridad en los teléfonos móviles solo se aceptará por el firmware del teléfono si se ha firmado por una clave certificada por una Autoridad de Certificación (clave raíz de CA). Además, los desarrolladores de terceras partes de aplicaciones y similares tendrán de vez en cuando claves y certificados para la creación de ciertos tipos de programas. Por lo tanto es deseable si estos temas relacionados con la seguridad se pudiesen gestionar en un nivel del teléfono móvil específico para teléfonos móviles individuales, en lugar de exclusivamente en el nivel de usuario (por ejemplo, el desarrollador).

En el pasado, normalmente no ha sido posible impedir de forma eficaz que un propietario o poseedor de un teléfono móvil reemplace el código dentro de ese teléfono móvil. La única protección ofrecida por los teléfonos móviles en el pasado ha sido con respecto a la sustitución remota de código, particularmente mecanismos para impedir que agresores remotos cambien el código en los teléfonos. Sin embargo, como se ha señalado, no ha habido buena protección para impedir que los usuarios de teléfonos móviles cambien el código dentro del teléfono. Desde un punto de vista práctico, solo se ha debido a la oscuridad del diseño de los teléfonos móviles y la confidencialidad de los mecanismos dentro de los teléfonos lo que ha hecho que los teléfonos móviles sean relativamente difíciles de atacar por el usuario del teléfono. Desafortunadamente, tales mecanismos también hacen difícil al fabricante del teléfono permitir específicamente que ciertas terceras partes tengan acceso al menos a porciones del código dentro del teléfono.

En particular, en muchos casos a un usuario o algunas otras terceras partes les gustaría reemplazar el código en un teléfono móvil con otro código para evitar algunos mecanismos de seguridad. Por ejemplo, los usuarios podrían querer reemplazar la información conocida como la Identidad del Equipo de estación Móvil Internacional (IMEI) que es un procedimiento normalizado de los fabricantes de equipos para identificar una estación móvil similar a una identificación del número de serie. De este modo, un usuario podría querer reemplazar el código IMEI en el teléfono para realizar servicios ilegales con ese teléfono (tal como la realización de llamadas telefónicas sin pagar). Al mismo tiempo, los fabricantes del teléfono móvil deben poder escribir el código y comprobar ese código para desarrollar sus productos de forma eficaz. De este modo, el fabricante del teléfono móvil puede querer que el código tenga ciertas modificaciones usadas y/o comprobadas por un grupo especial de usuarios con respecto a teléfonos móviles particulares.

En el pasado, la rebaja del nivel de seguridad de un teléfono móvil particular se ha conseguido usando alguna clase de conmutador hardware u otra operación hardware. Este tipo de mecanismo no se puede usar para proteger de forma eficaz frente a la manipulación del teléfono por el propietario o poseedor del teléfono. Además, tal mecanismo tiende a soportar solo un nivel grueso de control de seguridad tal como una funcionalidad de apagado / encendido.

Sería ventajoso permitir a ciertas terceras partes, tales como los desarrolladores de software, tener acceso a teléfonos móviles específicos con respecto a la carga de nuevo código software en los mismos, así como tener ese software instalado en el teléfono y la posibilidad de ejecutarlo más tarde sobre el teléfono. Es a estas capacidades deseadas a lo que se dirige la presente invención.

La Solicitud de Patente de los Estados Unidos US 2001/0021928 de Ludwing y otros desvela el uso de certificados de funciones para autorizar las transacciones dentro de una red de ordenadores.

El documento "Móbile agents protection in the Internet environment", de A. Corradi, R. Montanari, en los Procedimientos de la Vigésima Tercera Conferencia Anual Internacional de Software de Ordenadores y Aplicaciones, COMPSAC '99, desvela SOMA, un paradigma para la gestión de permisos de ejecución de Agentes Móviles en una red usando certificados de funciones.

La presente invención se dirige a la resolución de estos temas específicos.

Sumario de la invención:

La presente invención se dirige a un procedimiento y un aparato para permitir a al menos una parte la realización de ciertas actividades con respecto a un dispositivo, en donde el dispositivo tiene un certificado de función incorporado en el mismo, y en el que además ese certificado de función especifica al menos cierta actividad que se puede activar dentro del dispositivo por al menos una parte. En particular, la invención está dirigida a certificados de funciones para teléfonos móviles de modo que controlan el acceso al nivel de seguridad por el firmware del teléfono asociado. De este modo el teléfono móvil se controla en base a un teléfono individual.

En una implementación, el certificado de función controla la aceptación del código del ordenador para su uso en un teléfono móvil específico. El código de ordenador puede ser un código de prueba, un código de producción o cualquier tipo de código especial para alguna operación. El certificado de función en esta situación indica qué tipo o tipos de código se pueden descargar, instalar y/o ejecutar sobre un teléfono móvil, determinando de este modo las posibles funciones que puede adoptar el teléfono. El certificado de función puede indicar no solo los tipos de códigos que se pueden descargar al teléfono sino que también puede indicar que tal código se escribe (o se suministra) por un individuo específico o grupo, también identificado por el certificado de función. Los diferentes certificados de funciones en el mismo teléfono pueden proporcionar diferentes actividades a realizar sobre el teléfono por las diferentes entidades. Por lo tanto se consigue una gran flexibilidad mediante el uso de estos certificados de funciones.

Otra aplicación del certificado de función es controlar las facilidades de depuración asociadas con un teléfono móvil. Tales facilidades de depuración se pueden constituir dentro de un teléfono o conectarse a un teléfono a través de un puerto.

Los certificados de función los controla a su vez una Autoridad de Certificación y de este modo los certificados se pueden distribuir a terceras partes para permitir a las terceras partes la realización de operaciones específicas sobre un teléfono móvil. Por ejemplo, los certificados de funciones se pueden distribuir a desarrolladores de software de terceras partes de modo que permitan a estos desarrolladores ejecutar la depuración de bajo nivel del código sobre teléfonos móviles específicos usados para depuración. Tal distribución del certificado de función normalmente sería mediante la agrupación de certificados para el desarrollador con un equipo de desarrollo software (SDK). El certificado de función también se podría incorporar dentro del dispositivo en el momento de la fabricación o más tarde por la entidad que genera el certificado de función (normalmente una CA raíz).

Para verificar el certificado de función, el teléfono móvil almacena además la información relativa a la clave pública correspondiente a la clave privada usada por la CA para firmar el certificado de función. Esta información de clave pública es normalmente un valor de huella digital de una clave pública de CA. Como esta información de clave pública está en una parte de memoria resistente a la manipulación dentro del teléfono, solo un certificado de función correspondiente se puede verificar y usar en ese teléfono particular una vez que se recibe la clave pública de la CA.

Breve descripción de los dibujos

Para un entendimiento más completo de la naturaleza y los objetos de la presente invención, se hará referencia a la siguiente descripción detallada, tomada en conjunción con los siguientes dibujos en los que:

La Figura 1 es un diagrama de bloques de un dispositivo de teléfono móvil que soporta el uso de un certificado de función de acuerdo con la presente invención.

La Figura 2 es un diagrama de flujo que muestra las etapas para la implementación de un certificado de función para un dispositivo que permite a una tercera parte realizar al menos una actividad con respecto al dispositivo.

Mejor modo de realización de la invención

A medida que ha avanzado la infraestructura inalámbrica en todo el mundo, se ha hecho evidente que los teléfonos móviles necesitarán aumentar el número de funciones críticas de seguridad que pueden realizar. Tal funcionalidad puede incluir la firma de los datos, que presentan el contenido de protección usando la gestión de derechos digitales (DRM), y otras actividades de tipo similar. En el futuro, probablemente cada teléfono móvil tendrá una identidad permanente incorporada dentro del teléfono. Esta identidad se puede usar para impedir la modificación de la Identidad del Equipo de estación Móvil Internacional (IMEI) basada en la identidad que se usa ampliamente para identificar a los dispositivos móviles para los proveedores del servicio de la red inalámbrica. Además, los teléfonos móviles tendrán una clave secreta para su uso en la infraestructura de clave pública (PKI), La capacidad de firmar el código se usará en los teléfonos móviles para controlar la ejecución o instalación de un código de ordenador relacionado con la seguridad. La mayor parte de los códigos de ordenador críticos para la seguridad en los teléfonos móviles solo lo aceptará el firmware del teléfono si se ha firmado por una clave certificada por una Autoridad de Certificación (CA). Además, los desarrolladores de terceras partes tendrán, en muchas situaciones, claves y certificados para la creación de ciertos tipos de programas.

La presente invención se dirige al uso de un certificado de función específico de un teléfono móvil de modo que se controla el acceso al nivel de seguridad para ese teléfono móvil que impone el firmware del teléfono asociado. Tal certificado de función específico de un teléfono móvil proporciona un control de seguridad de un teléfono móvil individual. Aunque se dirige específicamente a teléfonos móviles, el procedimiento y el aparato de la presente invención generalmente son aplicables a cualquier dispositivo.

Es importante observar que tales certificados de funciones específicos de un teléfono móvil son diferentes de los certificados usados comúnmente en las infraestructuras de red. Normalmente los certificados de funciones se dan a una cierta entidad, tal como un usuario o un dispositivo, para autorizar a esa entidad a realizar alguna función para otros en base a una afiliación con la función. De este modo, un certificado de función tradicional podría autorizar a una tercera parte a crear un código de prueba para un teléfono móvil. Sin embargo, en el caso de un teléfono móvil, no debería permitirse a nadie crear un código de prueba para un teléfono arbitrario. De este modo la presente invención usa un certificado de función específico de un teléfono móvil (dispositivo) para permitir a otros realizar alguna actividad sobre un dispositivo específico, tal como un teléfono móvil. Cuando el dispositivo tiene un certificado de función tal como el usado para el desarrollo de teléfonos de prueba, los desarrolladores, incluyendo los desarrolladores de terceras partes, normalmente estarían autorizados para crear y ejecutar un código en ese teléfono específico de pruebas sin restricciones.

Refiriéndonos ahora a la Figura 1, se muestra un teléfono móvil específico **10** en un diagrama de bloques generalizado. En este se ve que contiene alguna forma de módulo de entrada / salida **12,** un puerto **13,** una unidad de procesamiento central (CPU) **14,** una memoria **16,** un firmware **18,** y una facilidad de depuración opcional **20.** El puerto **13** se puede conectar opcionalmente a una facilidad de depuración externa **20'**. Una tercera parte (TP) **22** también puede interactuar con el teléfono a través del puerto **13.**

El puerto **13** está conectado al módulo de E/S para comunicar con el mundo exterior. Este puerto puede ser una antena inalámbrica, un puerto de infrarrojos, un teclado, un conector (por ejemplo un puerto RS 232) y otra interfaz. La memoria incluirá normalmente al menos alguna memoria resistente a la manipulación **16'.** En la presente realización una Autoridad de Certificación (CA) emite un certificado de función y como bien se sabe en la técnica, tal certificado contendría diversos componentes tales como los enumerados en la Recomendación X.509 de la ITU-T, incluyendo el nombre de la Autoridad de Certificación que emitió el certificado, un número de serie, una fecha de expiración, así como otra información. En particular, el certificado de función contiene información relativa a una o más actividades permitidas. El certificado de función lo firma la CA que creó el certificado. Tal firma proporciona el mecanismo para permitir a una entidad (tal como un teléfono móvil u otro dispositivo) tener confianza en la autenticidad del certificado de función ya que el certificado de función se puede verificar solo con la clave pública correspondiente de la CA ligada a la clave privada de la CA usada para firmar el certificado de función. Una visión general de tales certificados se puede encontrar en el documento de Comunicaciones de Netscape titulado, "Introduction to Public-Key Cryptology" que se puede obtener de la Internet en la dirección http://developer.netscape.com/docs/manuals/security/pkin/contents.htm (última actualización del 9 de Octubre de 1998 en el momento de presentación de esta solicitud).

La clave pública de la CA normalmente se almacena en una porción de memoria resistente a la manipulación **16**'. Preferiblemente, se almacena una huella digital de la clave pública de CA en la memoria resistente a la manipulación. A continuación, la clave pública de la CA, que se puede enviar más tarde al dispositivo, se puede verificar por la huella digital de esta clave pública de CA recibida (usando el mismo algoritmo de huella digital usado para la huella digital inicial de la clave pública de CA) y comparar este valor de la huella digital con el valor almacenado en la memoria resistente a la manipulación. Si los valores de las huellas digitales coinciden, la clave pública recibida de la CA se autentifica y se puede usar para verificar el certificado de función. Los certificados de función normalmente se almacenan en la memoria 16.

De este modo una autoridad de seguridad de operación tal como un fabricante de teléfono móvil puede emitir los certificados de función, por ejemplo, a desarrolladores de software de terceras partes permitiendo que tales desarrolladores de software realicen ciertas actividades con respecto a teléfonos móviles específicos. El certificado de función se puede incorporar en la memoria del dispositivo en el momento que se fabrica el dispositivo o se puede descargar más tarde a través del módulo de E/S **12.** La clave pública de CA (o el valor de la huella digital de tal clave normalmente se almacenaría en la memoria resistente a la manipulación **16'** en el momento que se fabrica el dispositivo. Se observará que es posible, si se desea, generar certificados de funciones diferentes usando la misma clave privada de CA para la firma. En tal caso, se puede usar la clave pública de CA dentro de un dispositivo para verificar cualquiera de estos certificados de función.

Debería observarse que el certificado de función se usa normalmente con un dispositivo o posiblemente un grupo de dispositivos todos ellos asociados con la misma entidad. Por ejemplo se pude usar un certificado de función sobre un grupo de teléfonos móviles pertenecientes todos a una compañía específica. En cada caso, la clave pública (o preferiblemente el valor de la huella digital de la clave pública) correspondiente a la clave privada de la CA usada para firmar el certificado de función se almacena en una porción de memoria **16'** resistente a la manipulación en cada dispositivo.

El teléfono móvil, una vez recibido el certificado transmitido al mismo a través del módulo de E/S 12 (o almacenado anteriormente en el instante de la fabricación) intentaría, mediante la ejecución del código firmware asociado, verificar el certificado usando la clave pública de CA. Si se verifica, el teléfono determina qué actividades se pueden realizar sobre el mismo. Si el certificado de función se puede verificar usando la clave pública de CA, a continuación la actividad o las actividades especificadas sobre ese teléfono las puede realizar cualquier tercera parte (si no se identifican ninguna tercera parte en el certificado de función) o una tercera parte específica si se identifica esta en el certificado de función (véase más adelante).

La Figura 2 es un diagrama de flujo que muestra las diversas etapas para la realización de la generación y uso de los certificados de función específicos del dispositivo tales como para su uso con los teléfonos móviles. De este modo en la etapa 30, una Autoridad de Certificación (CA) genera un certificado de función para un dispositivo específico, tal como un teléfono móvil específico. El certificado de función se puede almacenar en la memoria en el momento que se fabrica el dispositivo o se puede distribuir a cualquier tercera parte para el uso de la tercera parte en una comunicación posterior con el teléfono móvil especificado.

Como se ve en la Figura 2, en la etapa 30, la Autoridad de Certificación (CA) genera un certificado de función con al menos una actividad permitida identificada dentro de ese certificado y que incluye opcionalmente la identidad de las terceras partes permitidas (TP) que pueden tener el derecho de realizar tales actividades con respecto al dispositivo o que tienen derechos con respecto a la descarga, la instalación y/o la ejecución del código en el dispositivo. En la etapa 32, la clave pública de CA (o preferiblemente el valor de la huella digital de esta clave pública), que corresponde a la clave privada de CA usada para firmar el certificado de función se almacena en el dispositivo en la memoria resistente a la manipulación 16'. El almacenamiento de la clave pública de CA (o valor de la huella digital) en la memoria 16' se puede hacer en cualquier momento antes o después de la generación del certificado de función. Se pueden almacenar una o más claves públicas de CA (o los valores de las huellas digitales de estas claves públicas) en el dispositivo en el área de memoria resistente a la manipulación y del mismo modo, se pueden generar uno o más certificados de función que pertenecen a un dispositivo específico. La clave pública de CA (o valores de la huella digital) se deberían almacenar en la memoria resistente a la manipulación 16' para impedir a las TP el intento de almacenar sus propias claves públicas en el dispositivo.

La memoria resistente a la manipulación **16'** significa alguna forma de memoria que se pueda interrogar para determinar si la información almacenada en la misma se ha modificado. El firmware 18 puede contener un código para conducir a la CPU **14** a realizar tal interrogación, o se puede realizar tal interrogación remotamente a través de una comunicación con el teléfono móvil, tal como a través del puerto **13.**

Se pueden usar otras formas de resistencia a la manipulación; tales como, la ofuscación del almacenamiento de información (o código) dentro del teléfono o el código del sistema operativo en el teléfono para resistir a los cambios de la memoria. Tales técnicas no se consideran tan eficaces como la memoria resistente a la manipulación 16'.

Como se ve en la etapa 34, el firmware **18** en el dispositivo lo ejecuta la CPU **14**. Una de las funciones del firmware es controlar la CPU para permitir que la CPU use la clave pública de CA (o el valor de la huella digital) almacenada en la memoria resistente a la manipulación **16'** para intentar verificar un certificado de función que se ha almacenado en el dispositivo o que lo ha recibido el dispositivo desde una tercera parte a través del módulo de E/S **12** y el puerto **13.** Si el valor de la huella digital de la clave pública de CA se almacena en la memoria resistente a la manipulación **16'**, a continuación el firmware causa que la CPU calcule la huella digital de la clave pública (tal como se recibe a través del puerto 13) usando el mismo algoritmo de huella digital usado para generar la huella digital inicial de la clave pública de CA, y por lo tanto para determinar si el valor de la huella digital coincide con el valor de la huella digital en la memoria resistente a la manipulación 16'. Si los valores de las huellas digitales son los mismos, entonces se usa la clave pública de CA para verificar el certificado de función (etapa 36).

En la etapa 36, se realiza una decisión concerniente a la verificación del certificado de función. Si se verifica, a continuación en la etapa 38 se analizan la información de actividad permitida, así como la identidad opcional de las terceras partes permitidas a partir del certificado. Esto también lo realiza la CPU **14** bajo la dirección del firmware **18**. Si no se verifica el certificado de función, entonces no se permite ninguna actividad con respecto al dispositivo (véase la etapa 40).

Si se identifican una o más terceras partes en el certificado de función, a continuación también es necesario que el firmware determine si la tercera parte que comunica con el dispositivo a través del módulo de E/S **12** coincide con al menos una tercera parte identificada en el certificado (etapa 42). Si se encuentra una coincidencia, a continuación se permite la actividad analizada en la etapa 38 con respecto a las terceras partes identificadas. Esto se muestra en la etapa 44. De lo contrario, no se permite ninguna actividad con respecto a las terceras partes no identificadas (véase la etapa 46).

Con respecto a la identificación de las terceras partes en el certificado de función, esto se puede hacer almacenando una clave pública de la tercera parte en el certificado y determinando más tarde si la clave pública recibida desde la tercera parte coincide con la que está dentro del certificado. El almacenamiento de la clave pública de la tercera parte preferiblemente se puede hacer almacenando una huella digital de la clave pública de la tercera parte y a continuación realizando una huella digital de la clave pública recibida desde la tercera parte (usando el mismo

algoritmo que se usó para almacenar el valor de la huella digital de la clave pública de la tercera parte en el certificado) de modo que se determina si las dos huellas digitales son idénticas. Si lo son, entonces se asume que la identidad de la tercera parte es correcta.

Si se permite a la tercera parte que realice actividades permitidas, las actividades se pueden dirigir a través del módulo de E/S **12** y el puerto **13.**

Se observará que el certificado de función puede identificar cualquier actividad permitida que se pueda realizar sobre el dispositivo, por ejemplo, tales actividades pueden proporcionar la aceptación del código de ordenador desde una tercera parte. De ese modo el certificado de función puede permitir la recepción del código de prueba desde una tercera parte y la instalación de ese código y/o su ejecución sobre el teléfono móvil. Como alternativa, el certificado de función puede proporcionar la aceptación del código de ordenador de producción, de nuevo con un permiso adicional de instalación y/o de ejecución de ese código sobre el teléfono móvil específico.

También se pueden proporcionar otros tipos de códigos especiales, dependiendo de las necesidades de desarrollo del teléfono. Dependiendo de la actividad o actividades a permitir sobre el teléfono móvil específico a la vista del certificado de función, puede ser necesario para el teléfono móvil interactuar adicionalmente con la tercera parte **22** (a través, por ejemplo, del puerto **13** - véase la Figura 1) para permitir las actividades a realizar, tales como, la recepción de datos o parámetros adicionales para su uso con respecto al código recibido.

Como se ve en la Figura 1, la actividad permitida también puede ser el uso de la facilidad de depuración **20** dentro del teléfono por la TP o para permitir a la TP el uso de una facilidad externa de depuración **20'** conectada al teléfono a través de por ejemplo el puerto **13**. De este modo se han descrito un aparato y un procedimiento flexible y relativamente seguro que permiten al fabricante de un dispositivo generar los certificados de función que cuando los lee el dispositivo proporcionan actividades permitidas específicas a realizar sobre el dispositivo. Por lo tanto el certificado de función es el vehículo para permitir a otros realizar tales actividades específicas solo sobre los dispositivos en los que el fabricante ha almacenado anteriormente su clave pública de CA necesaria para leer el certificado de función.

REIVINDICACIONES

1. Un procedimiento para permitir al menos a una parte realizar al menos una actividad permitida con respecto a un dispositivo (10) que comprende las etapas de:

incorporar un certificado de función en dicho dispositivo, en el que el certificado de función identifica dicha al menos una actividad permitida que se puede activar dentro del dispositivo y en el que el certificado de función lo genera una Autoridad de Certificación; e
incorporar la información relativa a una clave pública en dicho dispositivo, correspondiendo la clave pública a la clave privada usada por la Autoridad de Certificación para firmar el certificado de función, en el que el dispositivo está configurado para verificar el certificado de función usando dicha información relativa a la clave pública de la Autoridad de Certificación de modo que dicha al menos una actividad permitida la puede activar dentro del dispositivo dicha al menos una parte si se verifica el certificado de función.

2. Un procedimiento como se define en la reivindicación 1, en el que el certificado de función incluye información relativa a un control del nivel de seguridad para dicho dispositivo (10) de modo que el dispositivo (10) solo permite que dicha al menos una actividad permitida sea un tipo de acción que está dentro del nivel de seguridad del dispositivo tal como lo define el certificado de función.

3. Un procedimiento como se define en la reivindicación 2, en el que el nivel de seguridad definido por el certificado de función permite la descarga de un tipo de código software y/o su instalación y/o su ejecución en dicho dispositivo por dicha al menos una parte.

4. Un procedimiento como se define en la reivindicación 3, en el que el tipo de código software es del grupo de tipos de código software que consiste en un código de prueba, un código de producción y un código especial.

5. Un procedimiento como se define en la reivindicación 4, en el que el código especial puede ser un código enlazado con al menos una parte específica.

6. Un procedimiento como se define en la reivindicación 3, en el que el certificado de función contiene además información con respecto a una parte específica de dicha al menos una parte que puede descargar y/o instalar y/o ejecutar dicho tipo de código software.

7. Un procedimiento como se define en cualquiera de las reivindicaciones anteriores, en el que el certificado de función contiene además información con respecto a una parte específica de dicha al menos una parte que puede activar la al menos una actividad permitida dentro del dispositivo (10).

8. Un procedimiento como se define en la reivindicación 7, en el que dicha información con respecto a una parte específica es una huella digital de la información que identifica dicha clave pública de la parte específica, y en el que el dispositivo valida dicha parte específica recibiendo dicha información que identifica dicha clave pública de la parte específica, y calculando la huella digital de esta información y comparando el valor de la huella digital con el valor de la huella digital contenida en el certificado de función de modo que si los valores de las huellas digitales son iguales, entonces se permite que la parte específica active la al menos una actividad permitida.

9. Un procedimiento como se define en la reivindicación 7 o la reivindicación 8, en el que dicha parte específica es un grupo de entidades.

10. Un procedimiento como se define en cualquiera de las reivindicaciones anteriores, en el que la incorporación del certificado de función dentro del dispositivo se realiza después de que la información relativa a la clave pública de la Autoridad de Certificación se incorpore dentro del dispositivo (10).

11. Un procedimiento como se define en cualquiera de las reivindicaciones anteriores, en el que la información relativa a la clave pública de la Autoridad de Certificación se incorpora en el dispositivo (10) en un área resistente a la manipulación (16') de la memoria (16).

12. Un procedimiento como se define en la reivindicación 11, en el que el área resistente a la manipulación (16') de la memoria (16) se configura de modo que cualquier modificación de la información almacenada en la misma se puede comprobar.

13. Un procedimiento como se define en la reivindicación 1, en el que la actividad permitida es el uso de la facilidad de depuración (20) dentro de dicho dispositivo (10).

14. Un procedimiento como se define en cualquiera de las reivindicaciones anteriores, en el que la Autoridad de Certificación es una Autoridad de Certificación raíz.

15. Un procedimiento como se define en cualquiera de las reivindicaciones anteriores, en el que el dispositivo (10) es un dispositivo inalámbrico.

16. Un procedimiento como se define en cualquiera de las reivindicaciones anteriores, en el que el certificado de

función contiene cualquier limitación de uso con respecto a dicha al menos una actividad permitida.

17. Un procedimiento como se define en la reivindicación 16, en el que dicha cualquier limitación de uso incluye una limitación de tiempo con respecto a la activación de dicha al menos una actividad permitida.

18. Un procedimiento como se define en cualquiera de las reivindicaciones anteriores, en el que dicha información relativa a la clave pública de la Autoridad de Certificación es un valor de huella digital de dicha clave pública de la Autoridad de Certificación.

19. Un procedimiento como se define en cualquiera de las reivindicaciones anteriores, que comprende además la incorporación de al menos un certificado de función diferente en dicho dispositivo (10).

20. Un aparato para permitir al menos a una parte realizar al menos una actividad permitida con respecto al dispositivo (10), que comprende:

un medio para incorporar un certificado de función en dicho dispositivo, en el que el certificado de función identifica dicha al menos una actividad permitida que se puede activar dentro del dispositivo y en el que el certificado de función lo genera una Autoridad de Certificación;
un medio para incorporar información respecto a una clave pública en dicho dispositivo, correspondiendo la clave pública a la clave privada usada por la Autoridad de Certificación para firmar el certificado de función; y
un medio para configurar el dispositivo para verificar el certificado de función usando dicha información con respecto a la clave pública de la Autoridad de Certificación de modo que dicha al menos una actividad permitida la puede activar dentro del dispositivo dicha al menos una parte.

21. Un aparato como se define en la reivindicación 20, en el que el certificado de función incluye información con respecto al control del nivel de seguridad para dicho dispositivo (10) de modo que el medio para ejecutar el dispositivo dispone que la al menos una actividad permitida solo sea un tipo de acción que está dentro del nivel de seguridad del dispositivo (10) como lo define el certificado de función.

22. Un aparato como se define en la reivindicación 21, en el que el nivel de seguridad definido por el certificado de función permite la descarga de un tipo de código software a dicho dispositivo desde dicha al menos una parte.

23. Un aparato como se define en la reivindicación 22, en el que el tipo de código software es del grupo de los tipos de código software consistente en un código de prueba, un código de producción y un código especial.

24. Un aparato como se define en la reivindicación 23, en el que el código especial puede ser un código enlazado con al menos una parte específica.

25. Un aparato como se define en la reivindicación 23, en el que el certificado de función contiene además información con respecto a una parte específica de dicha al menos una parte que puede descargar y/o instalar y/o ejecutar dicho tipo de código software.

26. Un aparato como se define en cualquiera de las reivindicaciones 20 a 25, en el que el certificado de función contiene además información con respecto a una parte específica de dicha al menos una parte que puede activar la al menos una actividad permitida dentro del dispositivo (10).

27. Un aparato como se define en la reivindicación 26, en el que dicha información con respecto a una parte específica es una huella digital de la información que identifica dicha clave pública de la parte específica, y en el que el dispositivo (10) valida dicha parte específica al recibir dicha información que identifica dicha clave pública de la parte específica, y que calcula la huella digital de esta información y que compara el valor de la huella digital con el valor de la huella digital contenida en el certificado de función de modo que si los valores de las huellas digitales son iguales, entonces se permite que la parte específica active la al menos una actividad permitida.

28. Un aparato como se define en la reivindicación 32 o la reivindicación 33 en el que dicha parte específica es un grupo de entidades.

29. Un aparato como se define en cualquiera de las reivindicaciones 20 a 28, en el que la información relativa a la clave pública de la Autoridad de Certificación se incorpora en el dispositivo (10) en un área resistente a la manipulación de la memoria (16').

30. Un aparato como se define en cualquiera de las reivindicaciones 20 a 29, en el que dicha información relativa a la clave pública de la Autoridad de Certificación es una huella digital de dicha clave pública de la Autoridad de Certificación.

31. Un aparato como se define en la reivindicación 20, en el que la actividad permitida es el uso de una facilidad de depuración (20) dentro de dicho dispositivo (10).

32. Un aparato como se define en cualquiera de las reivindicaciones 20 a 31, en el que el dispositivo (10) es un dispositivo inalámbrico.

33. Un aparato como se define en cualquiera de las reivindicaciones 20 a 32, en el que el certificado de función contiene cualquier limitación de uso con respecto a dicha al menos una actividad permitida.

34. Un aparato como se define en la reivindicación 33, en el que dicha cualquier limitación de uso incluye una limitación de tiempo con respecto a la activación de dicha al menos una actividad permitida.

35. Un aparato como se define en cualquiera de las reivindicaciones 20 a 34, en el que los medios para la incorporación de un certificado de función en dicho dispositivo (10) se configuran además para incorporar al menos un certificado de función diferente en dicho dispositivo (10).

36. Un aparato como se define en cualquiera de las reivindicaciones 20 a 35, en el que dicho dispositivo (10) es un teléfono móvil (10).

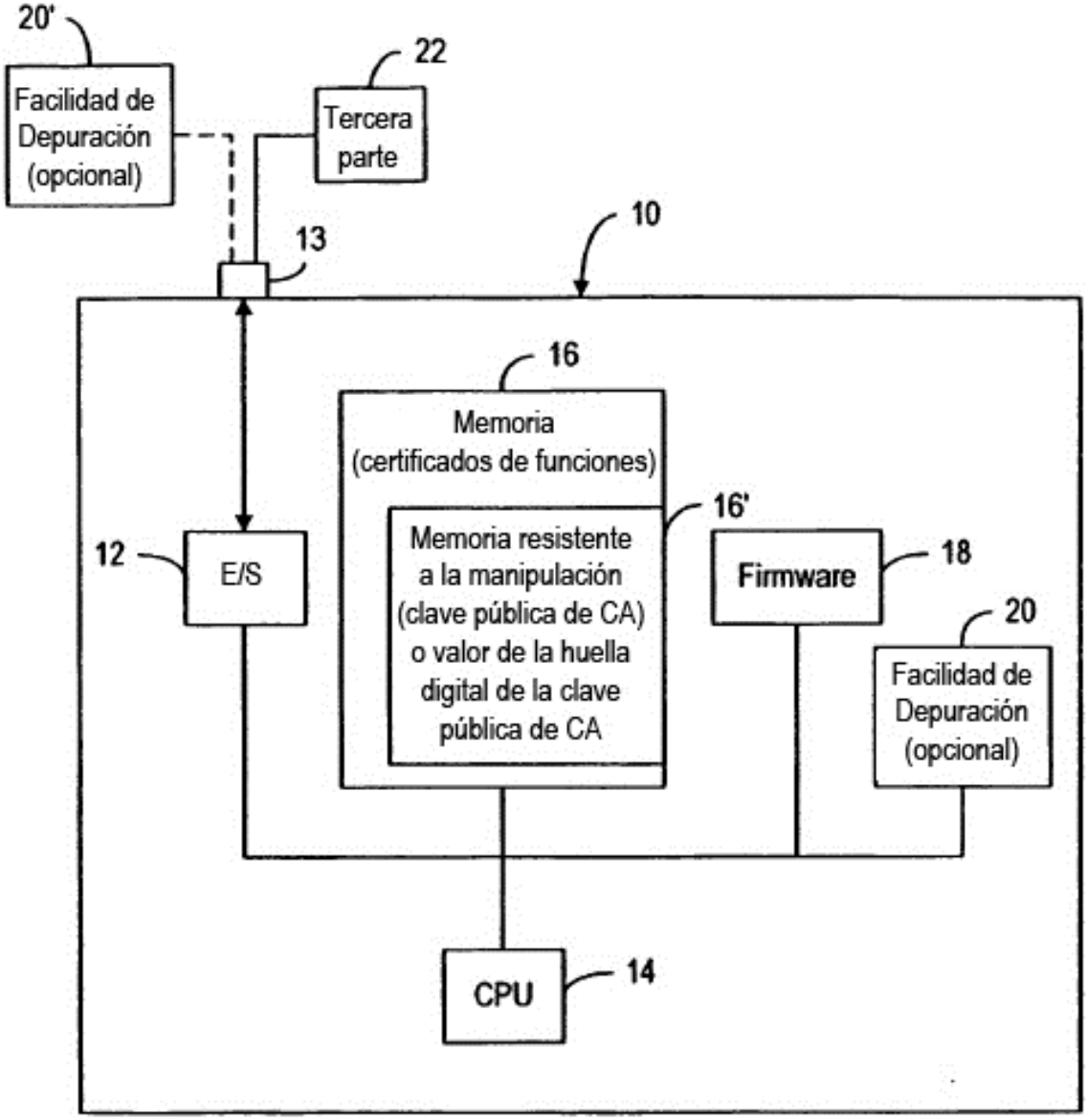
20'
Facilidad de Depuración (opcional)
22
Tercera parte
13
10
16
Memoria (certificados de funciones)
16'
Memoria resistente a la manipulación (clave pública de CA) o valor de la huella digital de la clave pública de CA
12
E/S
Firmware
18
20
Facilidad de Depuración (opcional)
CPU
14

FIG. 1

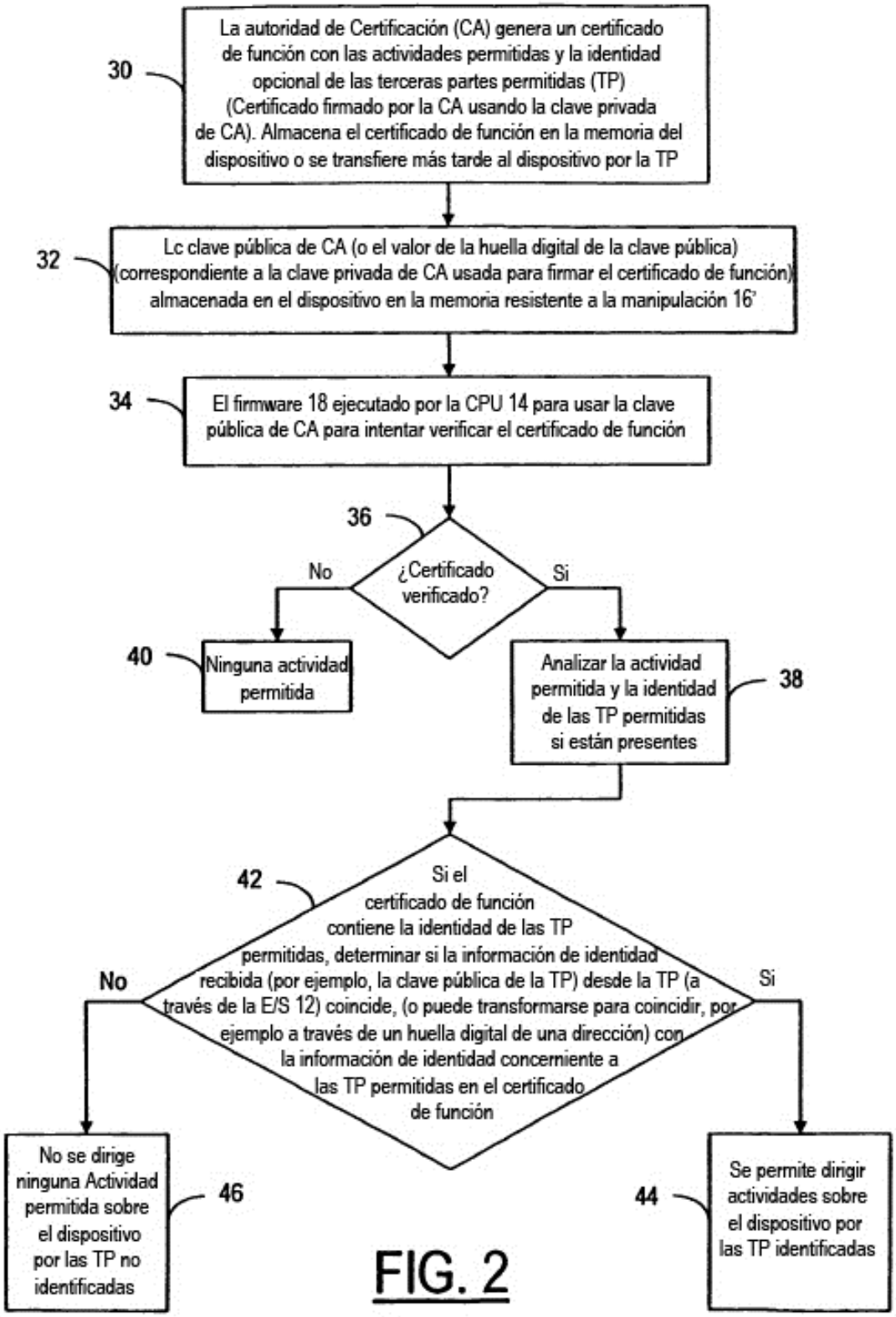
30
La autoridad de Certificación (CA) genera un certificado de función con las actividades permitidas y la identidad opcional de las terceras partes permitidas (TP) (Certificado firmado por la CA usando la clave privada de CA). Almacena el certificado de función en la memoria del dispositivo o se transfiere más tarde al dispositivo por la TP
32
Lc clave pública de CA (o el valor de la huella digital de la clave pública) (correspondiente a la clave privada de CA usada para firmar el certificado de función) almacenada en el dispositivo en la memoria resistente a la manipulación 16'
34
El firmware 18 ejecutado por la CPU 14 para usar la clave pública de CA para intentar verificar el certificado de función
36
¿Certificado verificado?
No
Si
40
Ninguna actividad permitida
38
Analizar la actividad permitida y la identidad de las TP permitidas si están presentes
42
Si el certificado de función contiene la identidad de las TP permitidas, determinar si la información de identidad recibida (por ejemplo, la clave pública de la TP) desde la TP (a través de la E/S 12) coincide, (o puede transformarse para coincidir, por ejemplo a través de un huella digital de una dirección) con la información de identidad concerniente a las TP permitidas en el certificado de función
No
Si
No se dirige ninguna Actividad permitida sobre el dispositivo por las TP no identificadas
46
44
Se permite dirigir actividades sobre el dispositivo por las TP identificadas

FIG. 2