(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 452 699**

(51) Int. CI.:

H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **22.06.2009 E 09768957 (4)**

(97) Fecha y número de publicación de la concesión europea: **12.02.2014 EP 2332284**

(54) Título: **Habilitación de un servicio en un equipo electrónico**

(30) Prioridad:

23.06.2008 DE 102008029636

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.04.2014

(73) Titular/es:

GIESECKE & DEVRIENT GMBH (100.0%)
Prinzregentenstrasse 159
81677 München, DE

(72) Inventor/es:

SPITZ, STEPHAN;
SCHERZER, HELMUT;
URHAHN, THORSTEN y
BORGS, HANS

(74) Agente/Representante:

ARPE FERNÁNDEZ, Manuel

DESCRIPCIÓN

Habilitación de un servicio en un equipo electrónico

La presente invención se refiere a un procedimiento para habilitar un servicio puesto a disposición por un equipo electrónico, a un equipo electrónico de este tipo y a un sistema que comprende un equipo electrónico de este tipo.

Para los soportes de datos portátiles y los equipos electrónicos móviles se conocen ya múltiples mecanismos de seguridad destinados a proteger la integridad del equipo y de los datos almacenados en el mismo, o la identificación unívoca del soporte de datos o su propietario.

La base técnica de tales mecanismos que protegen la integridad o hacen posible una identificación es con frecuencia un área de memoria especialmente protegida, para guardar en la misma a prueba de manipulación, por ejemplo datos de identificación. Existen por ejemplo mecanismos de aislamiento especiales que permiten configurar áreas de hardware y/o accesos a componentes de software de un equipo terminal para datos y procesos de nivel crítico de seguridad y separarlos eficazmente de las áreas correspondientemente desprotegidas, por ejemplo mediante soluciones de software, tales como procesadores virtuales seguros, o soluciones de hardware, tales como núcleos de seguridad dedicados. Dentro de un área protegida de este tipo pueden realizarse especialmente procesos de nivel crítico de seguridad, por ejemplo en un entorno de tiempo de ejecución seguro mediante un intérprete adecuado.

En la mayoría de los casos, por motivos de seguridad y puesta en práctica, los datos que conciernen a una individualización o identificación de soportes de datos portátiles se almacenan en el soporte de datos, por ejemplo en un área protegida de una tarjeta chip, una tarjeta inteligente o similar, durante el proceso de fabricación o al menos antes de la entrega del soporte de datos en cuestión a un usuario. Sin embargo, una individualización correspondiente de cualesquiera equipos terminales móviles en el marco de un proceso de fabricación lleva asociado un coste considerable debido a la infraestructura necesaria para ello y al menor rendimiento resultante.

Para la individualización de equipos terminales móviles se dispone en principio de procedimientos criptográficos, por ejemplo basados en una clave doble simétrica presente en el equipo terminal a individualizar, cuya clave pública es dotada de un certificado electrónico por una instancia de certificación fiable. Mediante una certificación, los compañeros de comunicación del equipo en cuestión que utilicen la clave pública del mismo para codificar o para comprobar una signatura del equipo se aseguran de que la clave pública procede realmente del equipo en cuestión y no ha sido sustituida por otra con fines de estafa.

En este contexto, el documento WO 2008/049959 A2 propone un procedimiento de certificación según la especificación PKCS ("Public Key Cryptography Standard [Norma de criptografía de clave pública]") en un entorno de radiotelefonía móvil con una tasa de transferencia y una seguridad de red posiblemente limitadas. El documento US 2005/0010757 da a conocer un procedimiento de certificación en una red distribuida, en el que, por motivos de seguridad, una petición de certificación de un nodo de red ante un servidor de certificación es posible sólo dentro de un intervalo de tiempo predefinido a partir de la inicialización del nodo de red correspondiente, lo que en relación con los equipos terminales móviles requeriría de nuevo una en sí impracticable individualización próxima a su inicialización usual en el marco de la fabricación. La entrada de una petición de certificado de un nodo de red dentro del intervalo de tiempo admisible se vigila por medio del instante de inicialización del nodo de red que el servidor de certificación tiene a la vista y la duración del intervalo de tiempo.

El documento WO 01/42889 A2 (D1) da a conocer el preámbulo de la reivindicación 1 y propone la utilización de certificados de arranque y certificados de software en un ordenador, para proteger el proceso de arranque en el ordenador. Los certificados de software utilizados son válidos sólo durante un espacio de tiempo limitado. Por lo tanto, el ordenador pide a un servidor un nuevo certificado cuando ha caducado el antiguo certificado de software.

El objetivo de la presente invención es poner a disposición una posibilidad segura, practicable y económica para la individualización de equipos terminales móviles electrónicos.

Este objetivo se logra según la invención mediante un procedimiento, un equipo electrónico y un sistema con las características de las reivindicaciones independientes. Las reivindicaciones dependientes de éstas describen configuraciones ventajosas y perfeccionamientos de la invención.

En un equipo electrónico, un servicio puesto a disposición pero aún no habilitado para su utilización – por ejemplo la ejecución por parte de un usuario del equipo – es habilitado mediante un proceso de registro ante un servidor de registro. Tal servicio a habilitar puede ser en principio cualquier ampliación de funciones o de recursos del equipo electrónico, en particular la habilitación de un funcionamiento individualizado en un equipo que antes no estuviera individualizado o de un área aislada protegida para la puesta a disposición de otras funcionalidades de seguridad del equipo terminal.

En lo que sigue se entiende por "registro" la comunicación de datos entre el equipo electrónico y el servidor de registro, mientras que, como resultado del registro, se denomina "habilitación" a la puesta a disposición propiamente

dicha del servicio en cuestión en el equipo para la utilización por parte del usuario. En este contexto, el equipo electrónico genera en el marco de un proceso de registro una petición de registro y envía ésta al servidor de registro, que en respuesta a la petición de registro recibida, genera una confirmación de registro y la envía de vuelta al equipo. Por último se habilita el servicio en cuestión en el equipo almacenando de una manera ya prevista la confirmación de registro recibida en el equipo.

Según la invención, una tercera instancia fiable establece un intervalo de tiempo para el proceso de registro anteriormente esbozado, de tal manera que sólo una petición de registro recibida dentro de dicho intervalo de tiempo es procesada por el servidor de registro y puede llevar a un registro del servicio en cuestión ante el servidor de registro. Así pues, el servicio en cuestión sólo puede habilitarse si la petición de registro se envía al servidor de registro dentro del intervalo de tiempo establecido; una petición de registro que llegue al servidor de registro fuera de este intervalo de tiempo (o incluso antes de que se establezca el intervalo de tiempo) al menos no recibe una confirmación de registro del servidor de registro. La instancia fiable puede en principio establecer el intervalo de tiempo con un instante de inicio y un instante de terminación cualesquiera, y por ejemplo también repetirlo periódicamente o algo similar.

Hasta aquí, el registro y la habilitación de un servicio dentro de un intervalo de tiempo establecido casi a voluntad pueden ser realizados por el equipo mismo con suficiente seguridad. Esto resulta ventajoso especialmente en el caso de los servicios cuyo habilitación en el marco del proceso de producción suponga un considerable gasto de recursos, por ejemplo en el marco de un proceso de inicialización de determinados servicios con un gran coste de tiempo, o que requieran una individualización del equipo electrónico en un entorno que en principio sea menos seguro que el ampliamente protegido entorno de producción. Además, la configuración del registro y la habilitación puede ser flexible, por ejemplo en función de especificaciones o modos de comportamiento del usuario de un equipo electrónico o del servicio mismo a habilitar, por ejemplo adaptando el intervalo de tiempo a un proceso de instalación o inicialización del servicio en el equipo.

Por consiguiente, un equipo electrónico según la invención comprende al menos suficientes recursos para la puesta a disposición de servicios, por ejemplo en forma de aplicaciones de software, en particular un procesador y una o varias memorias. Además, un equipo electrónico comprende una interfaz de comunicación de datos, que hace posible la comunicación de datos con el servidor de registro a realizar en el marco del proceso de registro, y un dispositivo de registro, que controla el proceso de registro y la habilitación final de un servicio mediante el almacenamiento de una confirmación de registro recibida. Según la invención, el dispositivo de registro está configurado de tal manera que la petición de registro se envía al servidor de registro dentro del intervalo de tiempo establecido por la instancia fiable en el servidor de registro, es decir que el dispositivo de registro tiene o recibe suficiente información sobre el intervalo de tiempo y luego concierta el proceso de registro.

El dispositivo de registro puede asegurar una petición de registro realizada a tiempo en el servidor de registro por ejemplo enviando una petición de registro automáticamente dentro de un intervalo de tiempo configurado en el dispositivo de registro ya durante la fabricación, configuración o inicialización del equipo, o enviando la petición de registro en respuesta a una información que defina el intervalo de tiempo procedente de la instancia fiable o el servidor de registro.

Un sistema de registro según la invención comprende por consiguiente un equipo electrónico, un servidor de registro y una instancia fiable, que respectivamente están configurados y cooperan de tal manera que un servicio puesto a disposición por el equipo electrónico pueda habilitarse según el proceso de registro antes descrito.

El servidor de registro es preferentemente un servidor central que ofrece una fiabilidad especial y que ha sido configurado y autorizado, por ejemplo por un fabricante del equipo electrónico o una entidad fiable similar, para efectuar el registro de servicios.

La instancia fiable puede ser por ejemplo un dispositivo de comunicación de un intermediario que venda equipos electrónicos según la invención o servicios a instalar y habilitar en tales equipos, o un instituto de crédito, una administración u otra instancia de este tipo. La fiabilidad de esta instancia o del dispositivo de comunicación correspondiente se crea mediante una autentificación ante el servidor de registro, por ejemplo criptográficamente o mediante una contraseña. De este modo, la fiabilidad del servidor de registro se extiende a la instancia, que con ello recibe autorización para establecer un intervalo de tiempo en el servidor de registro.

La instancia fiable puede comunicar al servidor de registro un intervalo de tiempo futuro mediante unas señales horarias correspondientes o bien arrancar el intervalo de tiempo de manera activa en el servidor de registro mediante una señal de inicio. En este último caso, el servidor de registro puede terminar el intervalo de tiempo al recibir una señal de parada o al transcurrir un tiempo predeterminado. La instancia fiable puede en particular establecer un intervalo de tiempo con un instante de inicio cualquiera tras la fabricación del equipo electrónico, por ejemplo tras la entrega del equipo electrónico a un usuario (por ejemplo por parte de la instancia fiable) o la instalación de un servicio a habilitar en el equipo electrónico.

La petición de registro generada por el dispositivo de registro comprende preferentemente una identificación unívoca del servicio a habilitar en cada caso, de manera que en particular existe la posibilidad de que el servidor de registro

pueda protocolizar y liquidar la habilitación de este servicio y, con ello, el tiempo de uso del mismo por parte de un usuario. Especialmente si el servicio a habilitar no se trata de una aplicación de software dedicada o similar, sino de una ampliación básica de funciones del equipo electrónico, también es posible integrar en la petición de registro una identificación unívoca del equipo electrónico en lugar de una identificación unívoca del servicio a habilitar (o adicionalmente a la misma). La información unívoca del equipo puede ser el número de serie del equipo. Esta información unívoca del servicio o del equipo puede ser utilizada por el servidor de registro también para, por medio de la identificación del servicio o del equipo que el servidor de registro tiene a la vista, reconocer o bloquear un nuevo intento de habilitación mediante una nueva petición de registro. Naturalmente, también es posible que una habilitación esté activa sólo durante un periodo de tiempo predeterminado, y que una vez transcurrido dicho intervalo de tiempo sea necesario realizar un nuevo registro/habilitación del servicio en cuestión. Esto también puede reconocerse y gestionarse por medio de una identificación del servicio o del equipo.

Los servicios a poner a disposición por el equipo que representan ampliaciones básicas de funciones del equipo electrónico pueden concernir, por ejemplo a la configuración de un área aislada protegida en el equipo que esté totalmente desacoplada, por lo que se refiere tanto al hardware como al software, de un área no protegida remanente del equipo electrónico, para almacenar en dicha área aislada datos relevantes para la seguridad y realizar en la misma procesos relevantes para la seguridad.

Por otra parte, tal ampliación básica de funciones del equipo electrónico puede consistir también, como ya se ha mencionado más anteriormente, en configurar un funcionamiento individualizado del equipo dotando al mismo, en el marco del proceso de registro, de una identificación individual verificable por terceros que permita averiguar sin lugar a duda la identidad del equipo.

Para habilitar tal funcionamiento individualizado del equipo electrónico, el dispositivo de registro del equipo electrónico puede por ejemplo dirigir a un servidor de certificación una petición de certificado que comprenda, al menos, una clave pública de una clave doble asimétrica existente en el equipo o generada por el equipo. Así pues, con la petición de certificado se presenta al servidor de registro configurado como servidor de certificación una solicitud de certificación de la clave pública del equipo electrónico, para transmitir así la fiabilidad del servidor de certificación a la clave pública.

Si el equipo electrónico pone una clave pública certificada a disposición de un compañero de comunicación para la protección criptográfica de mensajes o para la comprobación de una signatura criptográfica, el compañero de comunicación en cuestión puede verificar por medio del certificado si la clave pública que tiene a la vista corresponde realmente a la clave privada presente en el equipo electrónico. Por consiguiente, al entrar la petición de certificado, el servidor de certificación crea el certificado para la clave pública y envía el certificado de vuelta al equipo electrónico como confirmación de registro. Mediante el certificado, el equipo puede demostrar entonces su propia fiabilidad e identidad ante cualesquiera compañeros de comunicación, con lo que se hace posible un funcionamiento individualizado del equipo. El certificado comprende una firma que, de forma verificable por terceros, asocia la identificación del servicio o del equipo a la clave pública generada.

Así pues, la petición de registro comprende por regla general una identificación de servicio y/o una identificación de equipo. La confirmación de registro se crea para una identificación de servicio y/o una identificación de equipo, que se reciben con la petición de registro o bien se averiguan para la petición de registro. La confirmación de registro puede contener una signatura digital, que se forma mediante la identificación de servicio y/o la identificación de equipo y, en caso dado, mediante otros datos, como la clave pública generada.

Al menos la clave privada de la clave doble asimétrica y un eventual certificado de la clave pública recibido, se guardan preferentemente en un área protegida del equipo. Esta área protegida es preferentemente un área de hardware y software aislada a la que no puede accederse partiendo de una eventual área no protegida del equipo y que está separada de la misma. Un área aislada de este tipo puede presentar un entorno de tiempo de ejecución seguro con un intérprete correspondiente, para la realización de procesos de nivel crítico de seguridad, por ejemplo la generación de una clave doble asimétrica. En particular, la totalidad del proceso de registro descrito puede realizarse dentro de un entorno de ejecución seguro de este tipo, de manera que el dispositivo de registro puede ser una aplicación, una aplicación de sistema operativo, u otro componente de software del equipo electrónico, ejecutable como proceso por el entorno de tiempo de ejecución.

Un dispositivo de registro que crea y envía una petición de certificado y recibe y archiva el certificado está realizado preferentemente como cargador de arranque o como parte de un cargador de arranque de etapas múltiples del equipo electrónico. Si existe un área aislada protegida con un entorno de tiempo de ejecución seguro, un dispositivo de registro configurado como cargador de arranque puede en particular estar integrado en un proceso de arranque de etapas múltiples del equipo electrónico o del área protegida y del entorno de tiempo de ejecución seguro.

El funcionamiento individualizado del equipo electrónico se efectúa preferentemente en un primer proceso de arranque tras la entrega del equipo a un vendedor o usuario. Por supuesto, la habilitación de un servicio en el marco de un (primer) proceso de arranque puede estar prevista también para cualesquiera otros servicios, en particular también para ampliaciones básicas de funciones del equipo, por ejemplo la habilitación de un área aislada protegida en el equipo electrónico.

Otras características y ventajas de la invención se desprenden de la siguiente descripción de ejemplos de realización según la invención y otras alternativas de realización, en conexión con los dibujos adjuntos, que muestran:

Figura 1 un diagrama de flujo de un procedimiento según la invención;

Figura 2 un sistema de registro según la invención; y

Figura 3 una forma de realización especial de un dispositivo de registro según la invención.

La inicialización o individualización de un equipo electrónico 100, por ejemplo un equipo terminal (de telecomunicación) móvil, un sistema embebido, un sistema en chip (*System on a Chip*), o un soporte de datos portátil, como por ejemplo una tarjeta chip, una tarjeta de radiotelefonía móvil, una tarjeta multimedia segura o similar, puede realizarse mediante una infraestructura criptográfica por el método de que una clave pública de una clave doble asimétrica presente en el equipo electrónico sea certificada por una entidad preparada y autorizada para ello, por ejemplo un servidor de certificación 300. Además del equipo electrónico 100 y el servidor de certificación 300, el sistema de certificación ilustrado en las figuras 1 y 2 comprende una instancia fiable 200, por ejemplo un ordenador correspondientemente configurado de una administración u otra instancia fiable o similar.

En la figura 1 está esbozado el desarrollo del proceso de certificación realizado por el sistema de certificación. En primer lugar, el equipo electrónico 100 genera en la etapa S1 una clave doble asimétrica (GEN KEYPAIR), almacenándose en la etapa S2 la clave privada de la clave doble asimétrica en un área protegida 112, lo más segura posible contra la manipulación, del equipo electrónico 100 (SAVE PRIVKEY). Así, la clave privada está fijamente asociada al equipo electrónico 100, de manera que un mensaje codificado con la clave pública correspondiente por un compañero de comunicación del equipo electrónico 100 sólo puede ser decodificado por el equipo electrónico 100. El equipo electrónico 100 también puede, mediante la codificación de un mensaje con la clave privada, generar una signatura criptográfica, que permite al receptor de un mensaje enviado comprobar la procedencia de este último mediante la clave pública del equipo 100. Sin embargo, ambas cosas son posibles con una seguridad suficiente sólo si un compañero de comunicación del equipo electrónico puede partir del supuesto de que la clave pública presente realmente ha procedido del equipo electrónico en cuestión (es decir que el equipo electrónico tiene la correspondiente clave privada) y no ha sido sustituida por otra en el marco de un intento de estafa. En otras palabras: el equipo electrónico debe estar individualizado, es decir estar configurado para un funcionamiento individualizado.

La verificación de una asignación unívoca de la clave pública al equipo 100 puede asegurarse por el método de que la clave pública sea dotada por el servidor de certificación 300 de un certificado electrónico 305, es decir que se asigne de manera unívoca a la identidad del equipo electrónico 100. Un compañero de comunicación del equipo 100 que tenga a la vista la clave pública puede entonces comprobar, por medio del certificado 305, si la clave pública ha procedido realmente del equipo electrónico 100.

Con este fin, el equipo 100 genera en la etapa S3 una petición de certificación 114 que comprende al menos la clave pública a certificar y preferentemente también una identificación unívoca del equipo electrónico, por ejemplo su número IMEI (identidad de equipo móvil internacional) (GEN REQUEST). Sin embargo, el servidor de registro 300 acepta la petición de certificación 114 exclusivamente dentro de un intervalo de tiempo predeterminado y responde a la misma con el certificado 305 deseado, de manera que el equipo 100 no puede realizar la etapa S7 del envío de la petición de certificado 114 (SEND REQUEST) hasta que se haya iniciado el intervalo de tiempo correspondiente en el servidor de registro 300.

El intervalo de tiempo lo establece una instancia fiable 200 en el servidor de certificación 300. Con este fin, en primer lugar la instancia 200 se autentifica en la etapa S4 ante el servidor de certificación 300, por ejemplo criptográficamente o mediante una contraseña (AUTH), para que el servidor de certificación 300 certifique su fiabilidad y adquirir así la autorización para establecer el intervalo de tiempo. A continuación, mediante el envío de una señal de inicio 201 en la etapa S5 (START), se inicia el intervalo de tiempo en el servidor de certificación 300 en la etapa S6 (START TIMEFRAME). Una vez que el servidor de certificación 300 ha recibido tras el comienzo del intervalo de tiempo una petición de certificación 114 enviada en la etapa S7, el servidor de registro 300 genera en la etapa S8 un certificado 305 relativo a la clave pública recibida (GEN CERT) y envía el certificado 305 en la etapa S9 de vuelta al equipo electrónico 100 (SEND CERT).

En la etapa S10, el equipo 100 almacena el certificado 305 recibido preferentemente en la misma área protegida (SAVE CERT) en la que ya se había almacenado en la etapa S2 la clave privada, y en el futuro puede presentar a sus compañeros de comunicación potenciales su clave pública junto con el certificado 305 y demostrar así su identidad.

En la etapa S11, la identificación de equipo unívoca, por ejemplo el número IMEI, que ha recibido el servidor de certificación 300 en conexión con la petición de certificación 114 se almacena, para reconocer un nuevo intento de certificación del mismo equipo 100 y poder bloquearlo como intento de abuso (BLOCK IMEI), ya que toda petición de certificación posterior con una clave pública distinta puede considerarse como un intento de estafa. Como se ilustra en la figura 1, la terminación del intervalo de tiempo puede provocarla la instancia fiable mediante una señal de

terminación explícita 202 en la etapa S12 (END), terminándose acto seguido el intervalo de tiempo en la etapa S13 (END TIMEFRAME). También es posible que el intervalo de tiempo se termine de manera automática inmediatamente después de enviarse el certificado 305 al equipo electrónico 100 en la etapa S9 o que la instancia fiable haya transmitido ya al servidor de registro 300 en la etapa S5, en el marco de la señal de inicio 115, la duración del intervalo de tiempo, transcurrida la cual el servidor de registro 300 termina automáticamente el intervalo de tiempo.

En lo que se refiere a la coordinación entre el envío de la petición de certificado 114 en la etapa S7 y el inicio/la terminación del intervalo de tiempo en las etapas S5 y S12 pueden concebirse diversas variantes. Por una parte, el equipo 100 puede estar ya provisto de una información de tiempo correspondiente (por ejemplo almacenada ya durante la fabricación del equipo 100) sobre el intervalo de tiempo a iniciar en el servidor de registro 300 y, por lo tanto, no necesita una comunicación explícita sobre el inicio del intervalo de tiempo en la etapa S5. Por otra parte, también es posible que el equipo electrónico 100 sea informado bien por la instancia fiable 200 (en una etapa S5a) o bien por el servidor de registro 300 (en una etapa S6a) sobre el inicio del intervalo de tiempo y en caso dado sobre su duración o terminación.

La figura 2 describe más detalladamente la arquitectura de un equipo electrónico 100. El equipo electrónico 100 puede ser por ejemplo cualquier equipo terminal móvil, por ejemplo un equipo terminal de radiotelefonía móvil, un soporte de datos portátil, como por ejemplo una tarjeta chip, una tarjeta de radiotelefonía móvil o similar, un sistema embebido o un sistema en chip. Un equipo electrónico 100 de este tipo comprende en principio todos los recursos y componentes necesarios para ejecutar aplicaciones y servicios, en particular un procesador CPU 104, así como un dispositivo de almacenamiento compuesto de una memoria de trabajo RAM 101, una memoria regrabable Flash o EEPROM 102 y una memoria ROM 103 con un sistema operativo 115 (OS). El equipo 100 comprende además una interfaz de comunicación de datos 105 para la comunicación de datos con, al menos, el servidor de certificación 300.

El equipo electrónico 100 comprende preferentemente también un área aislada protegida 112 (TRUSTZONE), que constituye un área de la dotación de hardware y software del equipo electrónico 100 completamente separada mediante mecanismos de aislamiento, en particular una memoria RAM segura 107 (SEC RAM), para poder almacenar datos de nivel crítico de seguridad y realizar procesos de nivel crítico de seguridad en la misma. En particular se ejecuta en el área protegida 112 un entorno de tiempo de ejecución seguro 113 (RTE; *Runtime Environment*), que realiza procesos de nivel crítico de seguridad en la RAM segura 107. Mediante un dispositivo de registro 108, configurado preferentemente en el área protegida 112, se consigue una inicialización e individualización del equipo electrónico 100, o del área aislada protegida 112. El área protegida 112 puede aislarse del resto de los recursos del equipo electrónico 100 mediante tecnologías ya conocidas, por ejemplo mediante una virtualización en un sistema embebido o mediante un procesador autónomo seguro en el mismo chip que el procesador de aplicación 104 propiamente dicho.

En la forma de realización esbozada en la figura 2, el dispositivo de registro 108 del equipo electrónico 100 está realizado como cargador de arranque especializado 108 (cargador de arranque) (BOOT LOADER), que puede constituir por ejemplo una ampliación de gestores de arranque convencionales empleados para arrancar (*boot*) un sistema operativo de un medio de almacenamiento con secuencia de arranque o para arrancar (*boot*) un sistema embebido o cualquier otro equipo terminal móvil.

En esta forma de realización, todo el proceso de certificación es realizado por el cargador de arranque 108 en el marco del proceso de arranque del equipo 100, con lo que la certificación o individualización puede realizarse en un instante lo más temprano posible, pero no obstante arbitrario, tras la fabricación del equipo 100 o la entrega a un usuario. La individualización del equipo 100 se efectúa preferentemente en el marco del primer arranque del equipo 100. Por supuesto, el dispositivo de registro puede estar configurado también como un módulo de registro autónomo depositado en un área protegida de la memoria Flash 102 o como un módulo de sistema operativo 115 localizado en la memoria ROM 103, que se active en un instante cualquiera tras el arranque del equipo 100.

El cargador de arranque 108 genera y almacena la clave privada 109 (PRIV KEY) de la clave doble criptográfica en el área protegida de la memoria Flash 102. En ésta se almacena también el certificado 305 (CERT) recibido del servidor de registro 300. El cargador de arranque 108 envía a través de la interfaz de comunicación de datos 105 la petición de certificación 114 (REQUEST) al servidor de registro 300, que comprende al menos una interfaz de comunicación de datos 301, un procesador 302, una memoria 303 y un dispositivo de certificación 304 ejecutable por el procesador 302. El dispositivo de certificación 304 acepta la petición de certificación 114, genera el certificado 305 (CERT) y lo envía de vuelta al equipo electrónico 100, o a su cargador de arranque 108.

También a través de la interfaz de comunicación de datos 301, el servidor de registro 300 puede comunicarse con la instancia fiable 200, por ejemplo en el marco de una autentificación de la instancia fiable 200 ante el servidor de registro 300 y el subsiguiente establecimiento del intervalo de tiempo en el servidor de certificación 300 mediante señales de inicio y terminación 201, 202. La instancia fiable 200 puede representar en principio cualquier instancia intermedia entre el fabricante del equipo 100 y el usuario del equipo 100, por ejemplo un vendedor, un instituto de crédito, una administración o similar.

La figura 3 ilustra un proceso de arranque realizado por el cargador de arranque 108 dentro de la memoria RAM segura 107. El proceso de arranque esbozado en la figura 3 tiene varias etapas y es ejecutado por varios cargadores de arranque distintos, que arrancan preferentemente respectivos componentes del sistema distintos, por ejemplo el equipo electrónico 100 o su hardware y sistema operativo, el área protegida 112 y el entorno de tiempo de ejecución seguro 113. En el marco del arranque del área protegida 112, o del entorno de tiempo de ejecución seguro 113, la individualización del equipo electrónico 100 se realiza mediante una certificación ante el servidor de certificación 300. Así pues, el proceso de arranque de etapas múltiples usual realizado en conexión con un entorno de tiempo de ejecución seguro 113 se amplía con una inicialización o individualización criptográfica, que el cargador de arranque 108 realiza opcionalmente durante el primer arranque del equipo electrónico 100. A continuación se carga el sistema operativo 115 en la forma habitual en la parte no protegida de la memoria RAM 101.

Además de la individualización del equipo 100 descrita en conexión con las figuras 1 a 3, en principio pueden registrarse en el equipo 100, mediante un proceso de registro correspondiente ante un servidor de registro 300, y habilitarse en el equipo cualesquiera servicios. Un servicio tal a habilitar mediante un registro puede ser en particular también la utilización y configuración del área aislada protegida 112 o del entorno de tiempo de ejecución seguro 113, o también cualquier otra aplicación de software o recurso de hardware a disposición del usuario. Así, también es por ejemplo posible que una petición de registro 114 concierna a la habilitación de varios servicios y que la petición de registro incluya correspondientemente varias identificaciones de servicio, a las que el servidor de registro 300 puede responder a su vez de forma individual o conjunta. De forma correspondiente, el servidor de registro 300 bloquea entonces un nuevo registro de estos servicios.

La instancia fiable 200 puede establecer el intervalo de tiempo en el servidor de registro 300 de forma casi arbitraria, y no está limitada a un proceso de arranque del equipo 100 como el descrito en las figuras 2 y 3. Un intervalo de tiempo independiente del proceso de arranque del equipo 100 resulta conveniente especialmente si el servicio a habilitar no se trata de una ampliación básica de funciones, como la individualización criptográfica, sino de la habilitación de una o varias aplicaciones cualesquiera que, por ejemplo con fines de liquidación, deben registrarse ante el servidor de registro 300 antes de una ejecución en el procesador 104 del equipo 100.

Mediante una configuración correspondiente del intervalo de tiempo puede preverse un registro en cualquier instante (por ejemplo también según acuerdo con el usuario) para, por una parte, permitir al usuario del equipo electrónico una libertad de manejo máxima en lo que se refiere a los servicios utilizados y, por otra parte, satisfacer los requisitos de seguridad mediante el establecimiento de una limitación temporal mediante un intervalo de tiempo.

REIVINDICACIONES

1. Procedimiento para habilitar un servicio puesto a disposición por un equipo electrónico (100), que comprende las etapas:
- generación (S3) de una petición de registro (114) por parte del equipo (100) y envío (S7) de la petición de registro(114) a un servidor de registro (300);
- generación (S8) de una confirmación de registro (305) por parte del servidor de registro (300) y envío (S9) de la confirmación de registro (305) al equipo (100); y
- recepción de la confirmación de registro (305) por parte del equipo (100) y habilitación del servicio mediante almacenamiento (S10) de la confirmación de registro (305);
caracterizado porque
una instancia fiable (200) se autentifica (S4) ante el servidor de registro (300) y a continuación establece (S5, S12) un intervalo de tiempo en el servidor de registro (300), y la instancia fiable (200) establece (S5, S12) el intervalo de tiempo de tal manera que el servidor de registro (300) envía (S9) una confirmación de registro (305) sólo para una petición de registro (114) recibida dentro del intervalo de tiempo establecido, y porque el equipo (100) envía (S7) la petición de registro (114) al servidor de registro (300) dentro del intervalo de tiempo.

2. Procedimiento según la reivindicación 1, caracterizado porque, para establecer (S5, S12) el intervalo de tiempo, la instancia fiable (200) envía al servidor de registro (300) señales horarias (201, 202) que determinan un instante de inicio (S6) y un instante de terminación (S13) del intervalo de tiempo.

3. Procedimiento según una de las reivindicaciones 1 a 2, caracterizado porque la instancia fiable (200) puede establecer (S5) el intervalo de tiempo en cualquier instante de inicio (S6) tras la entrega del equipo (100) a un usuario.

4. Procedimiento según una de las reivindicaciones 1 a 3, caracterizado porque el equipo (100) genera (S3) una petición de registro (114) que comprende una identificación unívoca del servicio a habilitar, y el servidor de registro (300) protocoliza la habilitación del servicio por medio de la identificación unívoca.

5. Procedimiento según una de las reivindicaciones 1 a 4, caracterizado porque, como servicio a poner a disposición por el equipo (100), se habilita un área protegida (112) del equipo (100) o un funcionamiento individualizado del equipo (100).

6. Procedimiento según la reivindicación 5, caracterizado porque, para habilitar el funcionamiento individualizado, se genera (S3) como petición de registro una petición de certificado (114), que comprende al menos una clave pública de una clave doble asimétrica presente en el equipo (100) o generada por el equipo, y se genera (S8) como confirmación de registro un certificado (305) para la clave pública.

7. Procedimiento según la reivindicación 6, caracterizado porque el equipo (100) genera (S3) una petición de certificado (114) que comprende una identificación de equipo unívoca, y el servidor de registro (300) reconoce y bloquea (S11) una nueva petición de certificado del equipo (100) por medio de la identificación de equipo unívoca.

8. Procedimiento según la reivindicación 6 o 7, caracterizado porque en el equipo (100) está configurada un área protegida (112) con un entorno de tiempo de ejecución seguro (113) y en el área protegida (112) se almacenan (S2, S10) al menos una clave privada (109) de la clave doble asimétrica y el certificado (305).

9. Procedimiento según una de las reivindicaciones 5 a 8, caracterizado porque la habilitación del funcionamiento individualizado del equipo (100) es realizado por un cargador de arranque (108) del equipo (100), que se ejecuta en el marco de un proceso de arranque de etapas múltiples del equipo (100).

10. Procedimiento según una de las reivindicaciones 5 a 9, caracterizado porque el intervalo de tiempo se establece (S5, S12) de tal manera que la habilitación del funcionamiento individualizado del equipo (100) se realiza durante un primer proceso de arranque del equipo (100).

11. Equipo electrónico (100), que comprende un procesador (104) y una memoria (101, 102), para la puesta a disposición de un servicio, una interfaz de comunicación (105), para la comunicación de datos con al menos un servidor de registro (300), y un dispositivo de registro (108) que está configurado para provocar una habilitación del servicio generando una petición de registro (114), enviando la petición de registro (114) al servidor de registro (300) y almacenando una confirmación de registro (305) recibida del servidor de registro (300), caracterizado porque el dispositivo de registro (108) está configurado para enviar la petición de registro (114) al servidor de registro (300) dentro de un intervalo de tiempo establecido por una instancia fiable (200) en el servidor de registro (300), estando el equipo (100) configurado para ser informado por la instancia fiable (200), con o sin participación del servidor de registro (300), sobre el inicio del intervalo de tiempo.

12. Equipo (100) según la reivindicación 11, caracterizado porque el dispositivo de registro (108) está configurado para provocar una habilitación de un funcionamiento individualizado del equipo (100) generando una petición de certificado (114) que comprende al menos una clave pública de una clave doble asimétrica presente en el equipo (100) y almacenando un certificado (305) recibido del servidor de registro (300).

13. Equipo (100) según la reivindicación 12, caracterizado porque el equipo (100) es un equipo terminal móvil, un sistema embebido o un sistema en un chip, en el que está configurada un área protegida (112) con un entorno de tiempo de ejecución seguro (113), y el dispositivo de registro está realizado como un cargador de arranque (108) que está configurado para, en el marco de un primer proceso de arranque del equipo (100) y/o del área protegida (112), provocar la habilitación de un funcionamiento individualizado del equipo (100), almacenándose en el área protegida (112) la clave privada (109) de la clave doble asimétrica y el certificado (305) de la clave pública.

14. Sistema que comprende un equipo electrónico (100) según una de las reivindicaciones 11 a 13, un servidor de registro (300) y una instancia fiable (200), estando configurados y cooperando estos componentes del sistema de tal manera que un servicio puesto a disposición por el equipo electrónico (100) puede habilitarse de acuerdo con un procedimiento según una de las reivindicaciones 1 a 10.

FIG 1

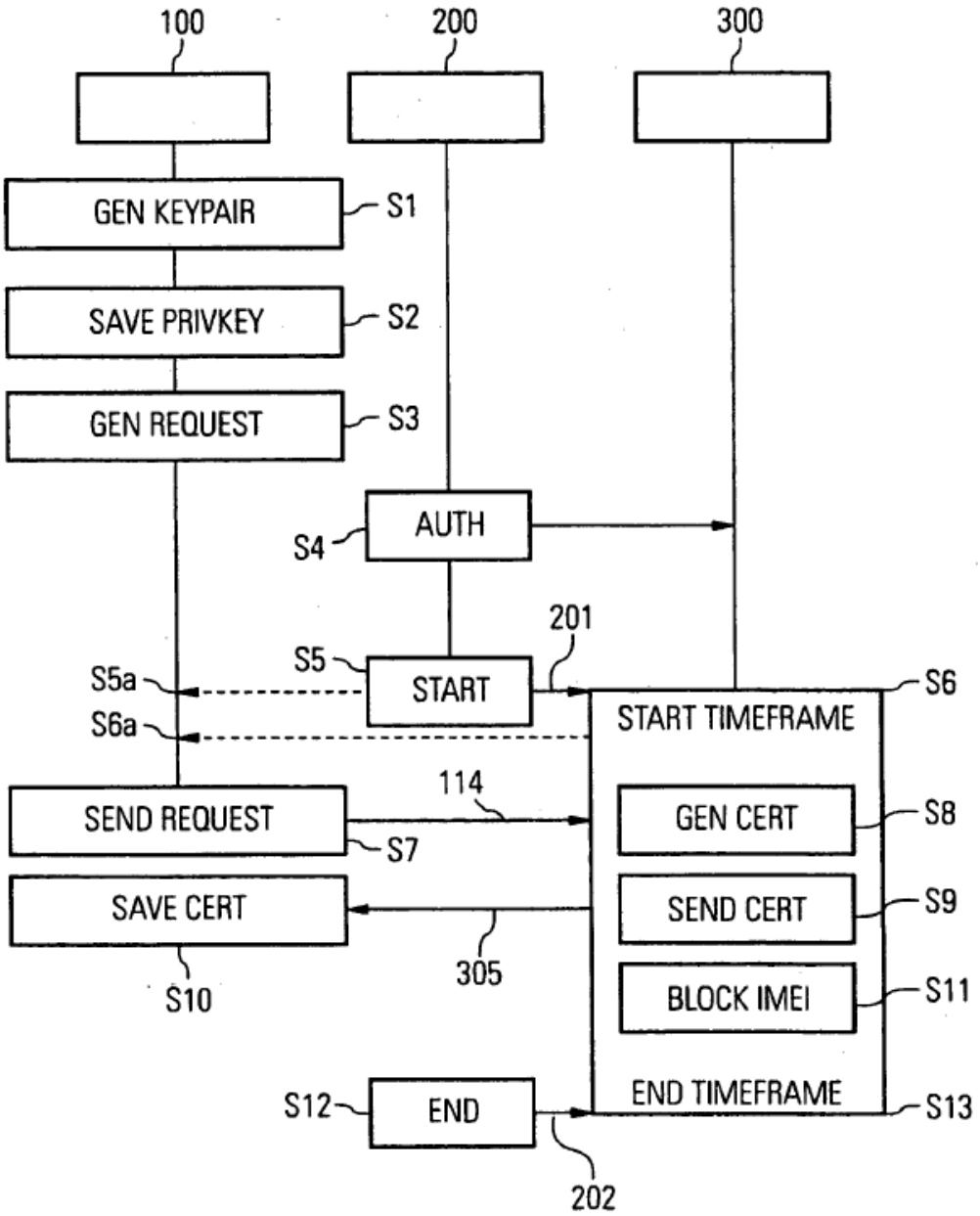

100
200
300
GEN KEYPAIR
S1
SAVE PRIVKEY
S2
GEN REQUEST
S3
AUTH
S4
201
S5
START
S5a
S6a
S6
START TIMEFRAME
114
SEND REQUEST
S7
GEN CERT
S8
SAVE CERT
SEND CERT
S9
305
BLOCK IMEI
S11
S10
END TIMEFRAME
S12
END
S13
202

FIG 2

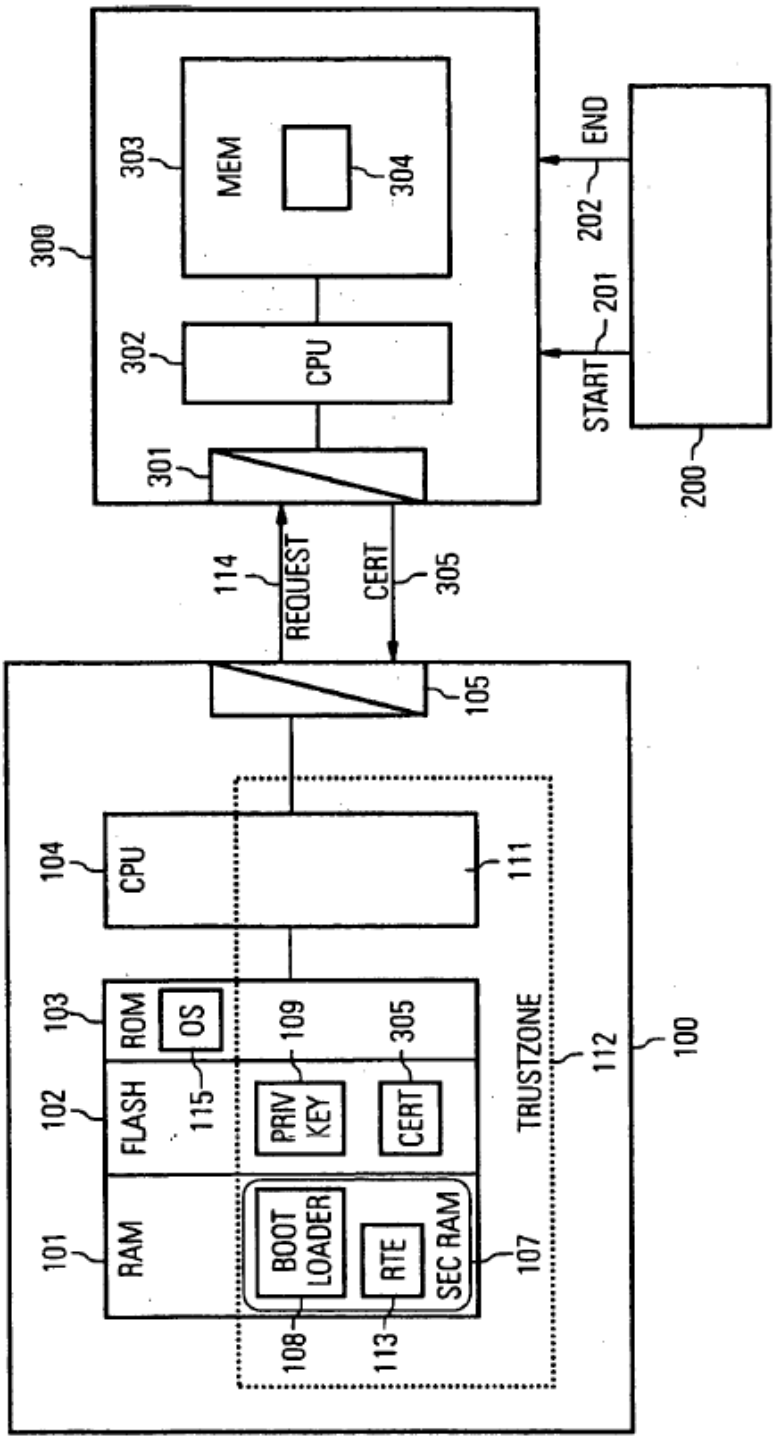
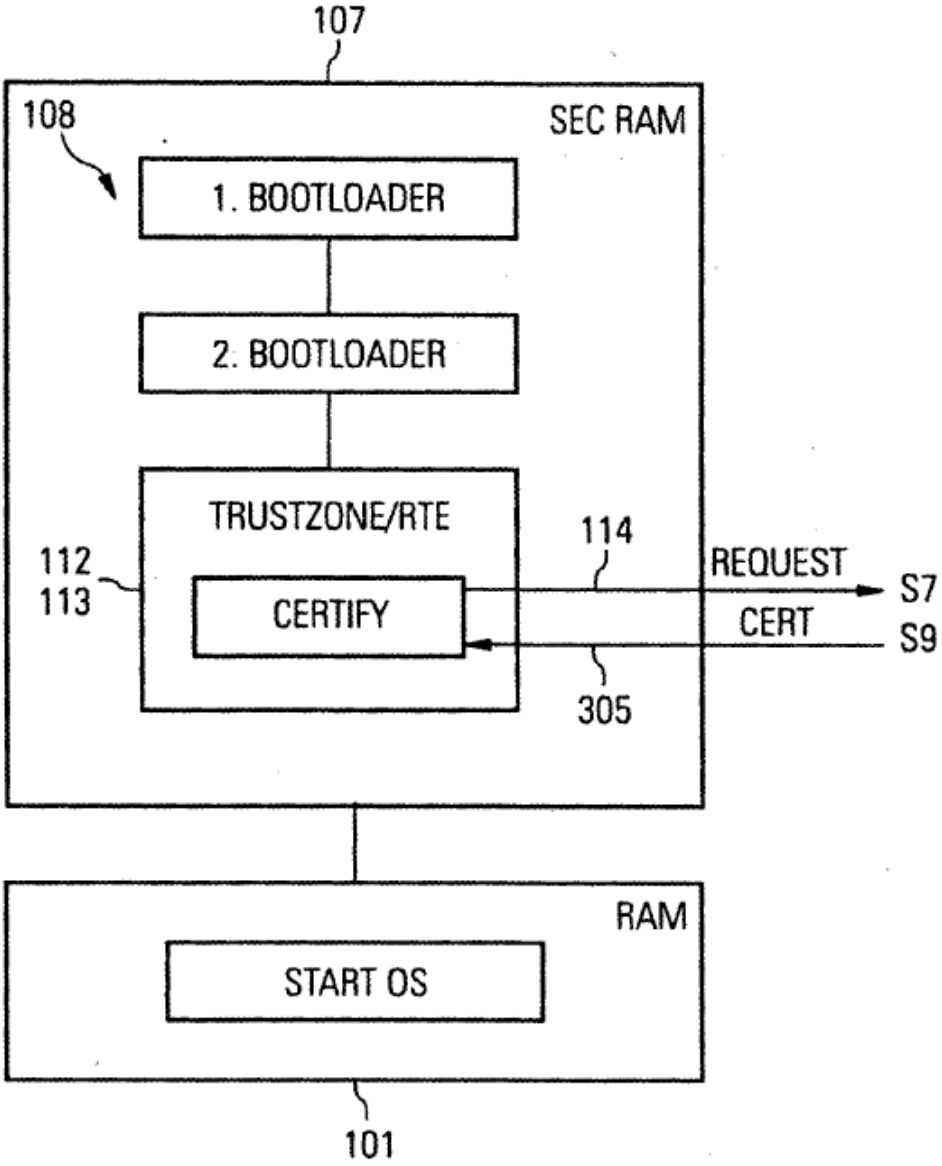

300
303
MEM
304
302
CPU
301
END
202
201
START
200
114
REQUEST
CERT
305
105
104
CPU
111
103
ROM
OS
109
305
102
FLASH
115
PRIV KEY
CERT
TRUSTZONE
112
100
101
RAM
BOOT LOADER
RTE
SEC RAM
107
108
113

FIG 3


107
108
SEC RAM
1. BOOTLOADER
2. BOOTLOADER
TRUSTZONE/RTE
112
113
CERTIFY
114
REQUEST
S7
CERT
S9
305
RAM
START OS
101

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

La lista de referencias citada por el solicitante lo es solamente para utilidad del lector, no formando parte de los documentos de patente europeos. Aún cuando las referencias han sido cuidadosamente recopiladas, no pueden excluirse errores u omisiones y la OEP rechaza toda responsabilidad a este respecto.

Documentos de patente citados en la descripción

- WO 2008049959 A2 **[0006]**
- US 20050010757 A **[0006]**
- WO 0142889 A2 **[0007]**