(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 558 008**

(51) Int. Cl.:
G06F 21/00 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **06.05.2011** **E 11865232 (0)**

(97) Fecha y número de publicación de la concesión europea: **18.11.2015** **EP 2705455**

(54) Título: **Determinación de la configuración de aparatos y datos de programación**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.02.2016

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karaportti 3
02610 Espoo, FI

(72) Inventor/es:

EKBERG, JAN-ERIK y
KAAJA, HARALD

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

ES 2 558 008 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Determinación de la configuración de aparatos y datos de programación

Campo técnico

La presente invención se refiere en general a la determinación de una configuración de un aparato y datos de programación. La invención se refiere en particular, aunque no exclusivamente, a la generación de los datos de programación y certificados de hardware para una memoria pasiva del aparato.

Técnica anterior

La fabricación de aparatos modernos, por ejemplo, terminales móviles, etc., requiere una programación permanente y/o temporal de componentes de memoria con cierta información. Dicha información puede comprender firmware, sistema operativo, software de aplicación o contenido multimedia, por ejemplo. El contenido multimedia puede comprender además, un conjunto de contenidos, un paquete de contenido o contenido seleccionado por el usuario, por ejemplo.

El software puede ser descargado a un aparato durante la fabricación, por ejemplo, la actualización se lleva a cabo mediante el uso de un mecanismo que requiere que algoritmos de actualización preliminares estén presentes en el aparato, una conexión física y una fuente de alimentación conectada. La descarga de software en productos se lleva a cabo convencionalmente en una estación de programación al final de la línea de fabricación después de que todos los componentes se han colocado en los productos. El software también puede ser reprogramado en fases posteriores. Existen también soluciones donde el software se programa en los chips de memoria en las estaciones de programación separadas antes de que un componente se coloque en la placa de circuito impreso (PWB).

El aparato puede ser suministrado a un número de diferentes variantes, dependiendo del firmware utilizado y la configuración del aparato. En algunos casos una variante del aparato solamente puede diferir en el tipo de software que controla el aparato.

En el caso de aparatos electrónicos, por ejemplo, el diseño físico del aparato puede ser el mismo para todas las variantes de un producto, pero algunas de las características básicas de control pueden funcionar de manera diferente. Normalmente, cada cliente del fabricante, normalmente un proveedor de servicios, un minorista, un operador o una nube, puede requerir un tipo de variante diferente que tiene características diferentes.

La reelaboración de variantes se ha convertido en una práctica común en la fabricación de productos de gran volumen, tales como aparatos móviles. Debido a las previsiones de ventas inexactas, grandes cantidades de una o más variantes pueden ser almacenadas en un centro de distribución como aumento de inventario. Los aparatos móviles creados de un tipo variante existentes pueden entonces necesitar ser convertidos rápidamente a una variante de otro tipo para su uso por otro proveedor de servicios.

Sin embargo, todos estos procedimientos convencionales implican ciertas desventajas. La etapa de programación solo se puede realizar en un tiempo predefinido en el proceso de fabricación, que también se aplica a cualquier tipo de prueba/depuración. Además, el enfoque convencional requiere que se realicen conexiones directas, es decir, cableadas, lo que requiere un equipo especial, lo que frena el ciclo de fabricación debido al tiempo requerido para establecer el contacto. Además, ninguna adaptación puede llevarse a cabo después de que el producto acabado se envasa, por ejemplo, actualizar el firmware o similar.

Convencionalmente, la etapa de programación para diferentes variantes solo se puede realizar en un tiempo predefinido en el proceso de fabricación. Además, el enfoque convencional requiere que se realicen las conexiones directas, es decir, cableadas, lo que requiere un equipo especial, lo que frena el ciclo de fabricación debido al tiempo requerido para establecer el contacto. Además, ninguna adaptación puede llevarse a cabo después de que el producto acabado se envasa, por ejemplo, actualizar el firmware o desea.

El documento US 2010132018 es técnica anterior adicional.

Sumario

La invención se define por las reivindicaciones independientes.

De acuerdo con un primer ejemplo aspecto de la invención, se proporciona un método que comprende:

la determinación de un identificador público para identificar una configuración de un aparato;
la determinación de un certificado de configuración común que comprende un identificador de certificado de configuración común para la verificación de los datos de programación;
la determinación de un certificado de hardware que comprende el identificador público y el identificador de

certificado de configuración común para asociar una combinación permitida de la configuración de aparatos y los datos de programación;
la generación de un paquete específico de los certificados de hardware correspondientes a las configuraciones de aparatos permitidos para ser proporcionadas;
el cifrado del paquete dedicado de los certificados de hardware utilizando una clave pública; y
el almacenamiento del paquete dedicado cifrado de los certificados de hardware con un identificador en una memoria pasiva del aparato.

El método puede comprender, además, definir el identificador para al menos uno de los siguientes niveles: un minorista, un operador y una nube. El certificado de configuración común puede estar firmado con una clave común. Un identificador de circuito integrado de aplicación específica se puede definir para el aparato y el certificado de hardware que comprende el identificador de circuito integrado de aplicación específica puede ser determinado. Además, el certificado de hardware puede estar firmado con una clave común.

Los datos de programación se pueden seleccionar entre el grupo que comprende:

firmware;
software del sistema operativo;
datos de configuración;
software de aplicación;
contenidos multimedia; y
controladores.

El método puede comprender, además, la definición de un identificador estático para identificar una configuración estática del aparato y que define un identificador dinámico para la identificación de una configuración dinámica del aparato. La configuración dinámica del aparato puede estar activa por un período fijo de tiempo. El paquete dedicado cifrado de los certificados de hardware puede ser transmitido de forma inalámbrica con el identificador a la memoria pasiva del aparato. La memoria pasiva del aparato puede comprender una etiqueta de memoria de radiofrecuencia (RF) incrustada accesible de forma inalámbrica y siendo alimentada desde un aparato externo.

De acuerdo con un segundo aspecto de ejemplo de la invención, se proporciona un método que comprende:

la detección de un paquete dedicado cifrado de los certificados de hardware de una memoria inalámbrica de un aparato basado en un identificador;
el descifrado del paquete dedicado cifrado de los certificados de hardware utilizando una clave privada;
la selección del certificado de hardware desde el paquete dedicado descifrado de los certificados de hardware correspondientes a una configuración deseada del aparato;
la escritura de datos de programación y el certificado de hardware seleccionado en la memoria pasiva del aparato; y
el borrado de certificados de hardware no seleccionados de la memoria pasiva del aparato.

El método puede comprender, además, la firma de los datos *de programación con una clave común que se utiliza para todas las combinaciones permitidas de la configuración* aparato y los datos de programación. Los datos de programación se pueden seleccionar entre el grupo que comprende:

firmware;
software del sistema operativo;
datos de configuración;
software de aplicación;
contenidos multimedia; y
controladores.

Un identificador estático puede ser detectado para identificar una configuración estática del aparato y un identificador dinámico se puede detectar para identificar una configuración dinámica del aparato. La configuración dinámica del aparato puede estar activa por un período fijo de tiempo.

El método puede comprender, además, transmitir de forma inalámbrica los datos de programación y el certificado de hardware seleccionado a la memoria pasiva del aparato. Además, la memoria pasiva del aparato puede comprender una etiqueta de memoria de radiofrecuencia (RF) incrustada accesible de forma inalámbrica y alimentada desde un aparato externo.

De acuerdo con un tercer aspecto de ejemplo de la invención, se proporciona un dispositivo que comprende:

al menos un procesador; y
al menos una memoria incluyendo el código de programa de ordenador, estando la al menos una memoria y el código de programa de ordenador configurados para, con el al menos uno procesador, hacer que el dispositivo al

menos lleve a cabo:

determinar, un identificador público para identificar una configuración del aparato;
determinar, un certificado de configuración común que comprende un identificador de certificado de configuración común para la verificación de los datos de programación;
determinar, un certificado de hardware que comprende el identificador público y el identificador de certificado de configuración común para asociar una combinación permitida de la configuración del aparato y los datos de programación;
generar, un paquete dedicado de los certificados de hardware correspondientes a las configuraciones de aparatos permitidos para ser proporcionados;
cifrar el paquete dedicado de los certificados de hardware utilizando una clave pública; y
almacenar el paquete dedicado cifrado de los certificados de hardware con un identificador en una memoria pasiva del aparato.

De acuerdo con un cuarto aspecto de ejemplo de la invención, se proporciona un dispositivo que comprende:

al menos un procesador; y
al menos una memoria incluyendo el código de programa de ordenador, estando la al menos una memoria y el código de programa de ordenador configurados para, con el al menos un procesador, hacer que el dispositivo al menos lleve a cabo:

detectar un paquete dedicado cifrado de los certificados de hardware de una memoria inalámbrica del aparato basado en un identificador;
descifrar el paquete dedicado cifrado de los certificados de hardware utilizando una clave privada;
seleccionar el certificado de hardware del paquete dedicado descifrado de los certificados de hardware correspondientes a una configuración deseada del aparato;
escribir los datos de programación y el certificado de hardware seleccionado en la memoria pasiva del aparato; y
borrar certificados de hardware no seleccionados de la memoria pasiva del aparato.

De acuerdo con un quinto aspecto de ejemplo de la invención, se proporciona un aparato que comprende:

al menos un procesador; y
al menos una memoria incluyendo el código de programa de ordenador, estando la al menos una memoria y el código de programa de ordenador configurados para, con el al menos un procesador, hacer que el aparato al menos:

reciba, usando la interfaz de comunicaciones de corto alcance inalámbrica, un paquete dedicado cifrado de los certificados de hardware con un identificador en la memoria pasiva;
transmita, mediante la interfaz de comunicaciones de corto alcance inalámbrica, el paquete dedicado cifrado de los certificados de hardware de la memoria inalámbrica basada en el identificador;
reciba, utilizando la interfaz de comunicación de corto alcance inalámbrica, datos de programación y un certificado de hardware seleccionado en la memoria pasiva; y
elimine certificados de hardware no seleccionados de la memoria pasiva basado en las instrucciones recibidas.

De acuerdo con un sexto aspecto de ejemplo de la invención, se proporciona un programa de ordenador incorporado en un medio legible por ordenador que comprende un código de programa ejecutable por ordenador, que cuando es ejecutado por al menos un procesador de un dispositivo, hace que el dispositivo lleve a cabo:

la determinación de un identificador público para identificar una configuración de un aparato;
la determinación de un certificado de configuración común que comprende un identificador de certificado de configuración común para la verificación de los datos de programación;
la determinación de un certificado de hardware que comprende el identificador público y el identificador de certificado de configuración común para asociar una combinación permitida de la configuración de aparatos y los datos de programación;
la generación de un paquete específico de los certificados de hardware correspondientes a las configuraciones de aparatos permitidos para ser proporcionados;
el cifrado del paquete dedicado de los certificados de hardware utilizando una clave pública; y
el almacenamiento del paquete dedicado cifrado de los certificados de hardware con un identificador en una memoria pasiva del aparato.

De acuerdo con un séptimo aspecto de ejemplo de la invención, se proporciona un programa de ordenador incorporado en un medio legible por ordenador que comprende un código de programa ejecutable por ordenador que, cuando es ejecutado por al menos un procesador de un dispositivo, hace que el dispositivo lleve a cabo:

la detección de un paquete dedicado cifrado de los certificados de hardware a partir de una memoria inalámbrica de un aparato basado en un identificador;
el descifrado del paquete dedicado cifrado de los certificados de hardware utilizando una clave privada;
la selección del certificado de hardware desde el paquete dedicado descifrado de los certificados de hardware correspondientes a una configuración deseada del aparato;
la escritura de datos de programación y del certificado de hardware seleccionado en la memoria pasiva del aparato; y
la eliminación de los certificados de hardware no seleccionados de la memoria pasiva del aparato.

Cualquier medio de la memoria anterior puede comprender un almacenamiento de datos digital, como un disco de datos o disquete, almacenamiento óptico, almacenamiento magnético, almacenamiento holográfico, almacenamiento optomagnético, memoria de cambio de fase, memoria de acceso aleatorio resistiva, memoria de acceso aleatorio magnética, memoria de electrolito sólido, memoria de acceso aleatorio ferroeléctrico, memoria orgánica o memoria de polímero. Se puede formar el medio de memoria en un aparato sin otras funciones sustanciales que memoria de almacenamiento o puede ser formada como parte de un aparato con otras funciones, incluyendo, pero no limitadas a una memoria de un ordenador, un conjunto de chips, y un subconjunto de un aparato electrónico.

Se han ilustrado diferentes aspectos de ejemplos no vinculantes y realizaciones de la presente invención en lo que antecede. Las realizaciones anteriores se utilizan simplemente para explicar aspectos o etapas seleccionados que pueden ser utilizados en las implementaciones de la presente invención. Algunas formas de realización pueden presentarse solamente con referencia a ciertos ejemplos de aspectos de la invención. Se debe apreciar que las realizaciones correspondientes se pueden aplicar también a otros aspectos de ejemplo.

Breve descripción de los dibujos

La invención se describirá, a modo de ejemplo solamente, con referencia a los dibujos adjuntos, en los cuales:

La figura 1 muestra algunos detalles de la arquitectura del sistema;
La figura 2 muestra un diagrama de relación, incluyendo los certificados de seguridad de acuerdo con diversas realizaciones de ejemplo de la presente invención;
La figura 3 muestra una estructura para un mecanismo de creación de paquete de certificado de hardware dedicado de acuerdo con un ejemplo de realización de la invención;
La figura 4 muestra algunos detalles de la determinación de los certificados de hardware y de datos de programación de acuerdo con un ejemplo de realización de la invención;
La figura 5 presenta un ejemplo de diagrama de bloques de un aparato y un dispositivo lector/grabador externo en el que pueden aplicarse diversas realizaciones de la invención;
La figura 6 ilustra un ejemplo de realización para un lector/escritor y una etiqueta de memoria de un dispositivo de radiofrecuencia incorporado (RF) de un aparato;
La figura 7 muestra un diagrama de flujo que muestra operaciones de acuerdo con un ejemplo de realización de la invención; y
La figura 8 muestra otro diagrama de flujo que muestra operaciones de acuerdo con un ejemplo de realización de la invención.

Descripción detallada

En la siguiente descripción, los números iguales indican los mismos elementos.

La figura 1 muestra algunos detalles de la arquitectura del sistema 100 de acuerdo con un ejemplo de realización de la invención. Un fabricante 110 fabrica aparatos, por ejemplo, equipos de usuario 120, para los minoristas 130-150 u operadores 160-180, por ejemplo. El equipo de usuario 120 puede comprender un teléfono móvil, un ordenador portátil, un asistente digital personal o una tableta de internet, por ejemplo.

De acuerdo con un ejemplo de realización de la invención, se proporciona la última personalización del hardware de equipo de usuario en una variante. Dicha variante puede ser objeto de un determinado operador o un modelo de aparato. Idealmente, la variante de emisión puede realizarse lo más tarde posible, incluso hasta en el almacén del operador 160-180, o en una oficina de ventas del minorista 130-150. Dicha emisión puede proporcionar flexibilidad en variantes de fabricación, pero también puede hacer posible la provisión de nuevas versiones de software, incluso las versiones de software de prueba, al equipo de usuario.

El equipo de usuario 120 puede ser enviado sin inicializar desde el fabricante 110 a los minoristas 130-150 y los operadores 160-180. Los almacenes de los minoristas 130-150 y de los operadores 160-180 pueden estar ubicados en todo el mundo. En el estado no inicializado, el equipo de usuario 120, incluso se puede intercambiar o ser revendido. El equipo de usuario 120 puede así ser enviado entre almacenes para equilibrar las variaciones de la oferta y la demanda. Solo cuando el aparato de equipo de usuario 120 se pone en uso, la variante de firmware puede ser proporcionada al aparato. La imagen de la variante de firmware puede incluso ser escrita en la memoria aparato cuando el aparato está apagado, potencialmente, incluso directamente a través del paquete de venta. Tal

actualización de firmware se puede utilizar con una tecnología inalámbrica de corto alcance, por ejemplo, el sistema de etiqueta de memoria de radiofrecuencia (RF). La actualización de firmware sin necesidad de apagar el aparato puede ahorrar en el coste de manipulación. Además, dicho enfoque puede ahorrar al fabricante 110 las estaciones de etiquetado de envío (es decir, un dispositivo de actualización) a los minoristas 130-150 y a los operadores 160-180 que permitirían el aprovisionamiento de firmware en la forma en que el equipo de usuario 120 se actualiza en las fábricas del fabricante 110.

Además, si el equipo de usuario 120 se cambia 165 desde un operador 160 al otro operador 170, las variantes de operador pueden ser reactualizadas de forma segura a firmware. Tal reactualización es posible si el equipo de usuario se suministra desde un dominio de operador a otro con la identificación de minorista o la identificación de operador apropiadas, por ejemplo. Además, si el equipo de usuario 120 se le permite ser independiente del minorista, puede ser alternativamente el mismo mecanismo utilizado para las variantes de imagen basadas en la nube con identificación de nube, por ejemplo.

Como se usa aquí, la frase "versión de software" puede referirse a una versión de una aplicación de software completa o simplemente una parte o componente de una aplicación de software. El término "certificado" como se usa en el presente documento puede referirse a cualquier bloque de datos firmados que puede estar firmado usando cualquier esquema conocido, como, por ejemplo, un esquema de clave privada/pública.

La figura 2 muestra un diagrama de relación, incluyendo los certificados de seguridad de acuerdo con diversas realizaciones de ejemplo de la presente invención. En este sentido, un certificado de hardware 205 y un certificado de configuración común 225 (generalmente referido como certificados de seguridad) se pueden incluir en un esquema para la gestión de versiones de software. En algunas realizaciones de ejemplo, la implementación del certificado de hardware 205 y el certificado de configuración común 225 permiten la actualización o la revisión de una versión de software. Además, en algunas realizaciones de ejemplo, la implementación del certificado de hardware 205 y del certificado de configuración común 225 también evita que el cambio a una versión de software más antigua o indeseable.

Ejemplo de realizaciones que emplean el certificado de hardware 205 y el certificado de configuración común 225 proporcionan un lazo seguro entre un identificador público único de un aparato y una versión de software particular para garantizar que una versión de software adecuada está siendo utilizada por el aparato. En este sentido, el certificado de hardware 205 puede estar más estrechamente asociado con el aparato y el certificado de configuración común 225 puede estar más estrechamente asociado con una versión de software. Una relación entre el certificado de hardware 205 y el certificado de configuración común 225, que puede ser autenticado de forma segura, puede facilitar la actualización de software en el aparato mientras que también proporciona características de seguridad.

En general, de acuerdo con algunas realizaciones de ejemplo, el certificado de configuración común 225 puede ser actualizada en un aparato cuando una versión actualizada del software se introduce en el aparato. Criterios de certificado de hardware 205 se pueden usar para verificar que el certificado de configuración común 225 es adecuado y por lo tanto verificar que la versión de software es adecuada para el aparato. Al determinar que una versión de software adecuada está instalada en el aparato, puede permitirse al software ser ejecutado por el aparato. En este sentido, una versión de software puede ser adecuada para un aparato no solo porque el software es una versión actualizada, sino también porque la versión de software es adecuada para la configuración particular del aparato (por ejemplo, variante del aparato).

En este sentido, la configuración particular del aparato puede ser identificada a través del identificador público único del aparato. Por ejemplo, el identificador público puede ser consultado en una base de datos que almacena información de configuración de los aparatos. Sin embargo, la implementación de la certificación de hardware 205 y el certificado de configuración común 225 puede facilitar la actualización de software de una manera tal que no es necesario exigir que el identificador público del aparato sea verificado para cada nueva instalación del software. Por el contrario, un proceso de autenticación de ejemplo entre el certificado de hardware 205 y el certificado de configuración común 225, utilizando criterios más generales que el identificador público único de un aparato, puede proporcionar para la actualización de las versiones de software sin la complejidad de involucrar al identificador público único en cada instalación de una nueva versión de software en el aparato. De esta manera, la fabricación de los aparatos se puede simplificar donde se va a instalar una nueva versión de software, debido a que cada instalación no necesita ser verificada a través del identificador público único.

Haciendo referencia de nuevo a la figura 2, el identificador público 200 puede ser un valor codificado o no modificable que reside en un dispositivo de hardware que es capaz de ejecutar una aplicación de software. El identificador público 200 puede almacenarse en un circuito integrado, tal como un dispositivo de memoria de solo lectura. En algunos ejemplos de realización, el identificador público 200 puede estar firmado y/o asociado con una clave privada. Además, el identificador público 200 puede ser único para el aparato asociado particular. Como tal, el identificador público 200 puede ser usado para identificar la configuración particular del aparato o de la variante del aparato.

La aplicación de software 245 puede ser cualquier aplicación de software para su ejecución por el aparato asociado con el identificador público 200. En algunas realizaciones de ejemplo, la aplicación de software 245 puede ser un sistema operativo para el aparato. La aplicación de software 245 puede tener y/o incluir una versión de software 250, que puede ser un número, una fecha, un tamaño (por ejemplo, el tamaño en kilobytes o similares), una combinación de los mismos, o similares. La versión de software 250 puede ser firmada y/o asociada con una clave privada para facilitar la autenticación segura de la aplicación de software 245. El certificado de hardware 205 puede ser único para un aparato de hardware (por ejemplo, un ordenador, un terminal móvil, o similar) y puede ser almacenado en la memoria del aparato. El certificado de hardware 205 puede estar asociado con o incluir un identificador público 210, un identificador de certificado de configuración común 215, y criterios de la versión del certificado de configuración común 220.

De acuerdo con un ejemplo de realización de la invención, el certificado de configuración común 225 puede estar asociado con un contenido 260. El contenido 260 puede ser cualquier contenido para ser utilizado por el aparato asociado con el identificador público 200. En algunos ejemplos de realización, el contenido 260 puede ser contenido multimedia para el aparato. El contenido 260 puede tener y/o incluir un identificador de contenido 265, que puede ser un número, una fecha, un tamaño (por ejemplo, el tamaño en kilobytes o similares), una combinación de los mismos, o similares. El identificador de contenido 265 puede estar firmado y/o asociado con una clave privada para facilitar la autenticación segura del contenido 260.

El identificador de contenido 265 pueden ser criterios utilizados para determinar si el contenido 260 es de una versión adecuada para un certificado de configuración común 225. El identificador de contenido 265 puede contribuir a un nivel adicional de seguridad para asegurar que el certificado de configuración común 225 no se utiliza en conjunción con un identificador de contenido inapropiado. Como tal, mediante el uso del identificador de contenido 265, el contenido inapropiado puede ser detectado y la ejecución del contenido puede ser prevenida. En algunas realizaciones de ejemplo, el identificador de contenido 265 puede incluir un valor de versión umbral para un contenido 260. El identificador de contenido 265 puede estar firmado y/o asociado a una clave privada para facilitar la autenticación segura.

El identificador público 210 del certificado de hardware 205 puede coincidir con el identificador público 200 de un aparato. La relación entre el identificador público 210 del certificado de hardware 205 y el identificador público 200 del aparato se puede usar para autenticar el certificado de hardware 205. En algunos ejemplos de realización, el identificador público 210 pueden estar firmado y/o asociado con una clave privada para facilitar la autenticación segura del certificado de hardware 205. El fracaso para autenticar el certificado de hardware a través del identificador público 210 puede impedir la ejecución de software en el aparato.

El identificador de certificado de configuración común 215 puede ser un valor que se puede utilizar en la autenticación de un certificado de configuración común 225. El fallo de autenticación de un certificado de configuración común 225 a través del identificador de certificado de configuración común 215 puede impedir la ejecución de software asociado con dicho certificado de configuración común. El identificador de certificado de configuración común 215 puede estar firmado y/o asociado a una clave privada para facilitar la autenticación segura del certificado de configuración común 225. Los criterios de la versión del certificado de configuración común 220 pueden ser criterios utilizados para determinar si un certificado de configuración común 225 es de una versión adecuada. En este sentido, los criterios de la versión del certificado de configuración común 220 pueden ser configurados de tal manera que los criterios pueden determinar si un certificado de configuración común 225 se asocia con el software o contenido que es de una versión adecuada y está configurado para una variante del aparato adecuada. La versión correcta puede ser una versión más reciente aplicación de software, el contenido incluido seleccionado fijado en el minorista, una versión limitada de una aplicación/contenido o una versión de prueba, por ejemplo. A través del uso de los criterios de la versión del certificado de configuración común 220, los certificados de configuración comunes inapropiados pueden ser detectados y la ejecución del software asociada con un certificado de configuración común apropiado puede prevenirse. En algunas realizaciones de ejemplo, los criterios de la versión del certificado de configuración común 220 pueden incluir un valor para la versión umbral de un certificado de configuración común 225. En este sentido, los certificados de configuración comunes con un valor de versión mayor o igual que el valor de la versión umbral pueden reunir por lo menos un aspecto de los criterios de la versión del certificado de configuración común 220. Los criterios de la versión de configuración común 220 pueden estar firmados y/o asociados con una clave privada para facilitar la autenticación segura antes de la aplicación de los criterios. El certificado de configuración común 225 puede estar asociado con una aplicación de software 245. En algunas realizaciones de ejemplo, un certificado de configuración común puede ser común entre todas las instalaciones de una aplicación de software particular. El certificado de configuración común 225 puede ser almacenado en la memoria del aparato. El certificado de configuración común 225 puede incluir un identificador del certificado de configuración común 230, una versión de certificado de configuración común 235, criterios de identificación de contenidos 255 y criterios de versiones de software 240.

El identificador de certificado de configuración común 230 puede ser un valor que se puede utilizar en la autenticación de un certificado de configuración común 225 con un certificado de hardware 205. En este sentido, en algunas realizaciones de ejemplo, si el identificador de certificado de configuración común 215 de un certificado de hardware coincide con el identificador certificado de configuración común 230 del certificado de configuración común

225, entonces el certificado de configuración común 225 puede ser autenticado. Un fallo de autenticación de un certificado de configuración común a través del identificador de certificado de configuración común 230 puede impedir la ejecución de software asociado con el certificado de configuración común. Similar al identificador de certificado de configuración común 215, el identificador de certificado de configuración común 230 puede estar firmado y/o asociado con una clave privada para facilitar la autenticación segura del certificado de configuración común 225.

Como se describió anteriormente, la versión del certificado de configuración común 235 se puede aplicar a los criterios de la versión del certificado de configuración común 220 de un certificado de hardware 205 para determinar si la versión del certificado de configuración común 235 satisface los criterios de la versión del certificado de configuración común 220. El fallo de la versión del certificado de configuración común para satisfacer los criterios de la versión del certificado de configuración común 220 puede resultar en la prevención de ejecución de software asociado con un certificado de configuración común. Similar a los criterios de identificador de certificado de configuración común 220, la versión del certificado de configuración común 235 puede estar firmada y/o asociada a una clave privada para facilitar la autenticación segura de la versión del certificado de configuración común 235. El certificado de configuración común 225 puede pertenecer a una determinada plataforma de certificado de configuración común. Además, la utilización de las formas de realización de la invención permite por lo tanto funcionalidades de gestión de plataforma.

Los criterios de la versión del software 240 pueden ser criterios utilizados para determinar si una versión de software 250 es de una versión adecuada para un certificado de configuración común 225. Los criterios de la versión del software 240 pueden contribuir con un nivel adicional de seguridad para asegurar que el certificado de configuración común 225 no se utiliza en conjunción con una versión de software apropiada. Como tal, mediante el uso de criterios de la versión de software 240, aplicaciones de software inapropiadas pueden ser detectadas y la ejecución de las aplicaciones de software puede ser prevenida. En algunos ejemplos de realización, los criterios de la versión de software 240 pueden incluir un valor umbral para la versión de una versión de software 250. A este respecto, las aplicaciones de software con un valor de versión mayor que o igual que el valor de versión umbral pueden satisfacer los criterios de la versión de software 240. Los criterios de la versión de software 240 pueden estar firmados y/o asociados con una clave privada para facilitar la autenticación segura antes de la aplicación de los criterios para una versión de software 250.

De acuerdo con un ejemplo de realización de la invención, las diferentes variantes pueden comprender variantes de aplicación, variantes de servicios (empaquetadas o separadas), variantes del operador, variantes de firmware, variantes de usuario, variantes del sistema operativo, variantes de nivel aparato, variantes de conjunto de aparato seleccionado por el usuario, variantes de la infraestructura, e incluso variantes de la nube.

Una variante del firmware puede ser entendida como una aplicación de software 245 en la figura 2, por ejemplo. La versión de la variante 250 se replica en el certificado de configuración común 225. La coincidencia entre las identidades, o versiones, en el certificado de configuración común 225 y la imagen de firmware 245 se comprueba en el arranque del aparato y tienen que ser las mismas. La razón fundamental de esta comprobación es que no se debe permitir al usuario cambiar la variante después de la compra. El certificado de configuración común 225 puede estar firmado con una clave común en todos los aparatos de un tipo específico. El certificado de configuración común 225 también puede tener el identificador de certificado de configuración común propio 230.

Además, el identificador de certificado de configuración común 230 se puede replicar en el certificado de hardware 205 que puede unir de forma única las identidades en el aparato al identificador público 210. El identificador público 210 puede ser, por ejemplo, un identificador de circuito integrado de aplicación específica único (ASIC id). El certificado de hardware 205 puede contener el identificador del certificado de configuración común 230 y la aplicación del identificador de circuito integrado específico (ASIC id) 210, firmado con una clave común a través de la plataforma de hardware. La coincidencia de las identidades puede comprobarse al arrancar el aparato.

En el caso que haga falta el aprovisionamiento de imágenes postfábrica y siempre y cuando la variante no cambie de la prevista originalmente, se puede hacer la reactualización de la imagen de variante. Esto significa que las actualizaciones de imagen se pueden realizar.

En general, decidir la variante en una etapa muy tardía antes de que el aparato termine en el cliente trae el problema introducido por la existencia del certificado de hardware 205. Puesto que el certificado de hardware 205 puede estar unido al circuito integrado de aplicación específica (ASIC) del aparato, y a través del certificado de configuración común 225 puede también unir el tipo de variante, se necesita dicho certificado para cualquier posible tipo de variante con la que el aparato potencialmente podría terminar.

Una posible solución podría ser la de incluir certificados de hardware 205, para todas las posibles variantes para este hardware, en el aparato. Esto puede dar lugar a una solución de trabajo, pero permite al usuario final (o cualquier entidad que ha manejado el aparato entre la fábrica y el cliente final) cambiar la variante del aparato a cualquier otra variante disponible para ese hardware del aparato. Otra posible solución podría ser la de incluir un protocolo de acondicionamiento activo a los servidores fabricante que generan el correspondiente certificado de

hardware 205 para el aparato bajo demanda, cuando se presenta con el identificador público 200 del aparato. Esta solución requiere un canal abierto entre los almacenes de todo el mundo y el acondicionamiento de seguridad del fabricante. También se requiere una confianza en la entidad de actualización, ya que el fabricante debe hasta cierto punto confiar en el identificador público 200. El operador o el minorista pueden tener un certificado autorizado para actualizar o un dispositivo de actualización autorizada, por ejemplo.

De acuerdo con un ejemplo de realización de la invención se proporciona un sistema seguro para el aprovisionamiento de la variante (y con ello la imagen de la variante) para el aparato. El aprovisionamiento puede realizarse en una etapa tardía, por ejemplo, en los locales del operador. El sistema puede ser implementado con distintos niveles de seguridad y con el mecanismo de borrado de todos los otros conjuntos de cifrados de los certificados de hardware 205 de la memoria del aparato después de escribir la imagen de la variante deseada. El aprovisionamiento se puede utilizar a nivel de aparato, a nivel de infraestructura o en el nivel de la nube, diferenciando la selección de variante de forma segura. Los certificados de hardware permitidos 205 con identificadores del minorista, identificadores del operador y los identificadores de la nube podrán almacenarse en la memoria del aparato en la fase de fabricación y los certificados de hardware no utilizados podrán ser eliminados cuando se pone el aparato en funcionamiento.

La figura 3 muestra una estructura para un aparato de creación del paquete de certificado de hardware dedicado de acuerdo con un ejemplo de realización de la invención. De acuerdo con un ejemplo de realización de la invención, los operadores y los minoristas se pueden identificar a los servidores de seguridad del fabricante. Dicha identificación se acompaña con una clave de operador/minorista pública (PKOx) 315 y posiblemente con un certificado de acompañamiento describiendo la validez de la clave (no se muestra). La clave pública del operador 315 puede ser acordada como parte de un proceso de certificación, pero una alternativa es que el fabricante proporcione tarjetas inteligentes a los operadores con la correspondiente clave de operador privada (SKOx) 325 en la tarjeta.

De acuerdo con un ejemplo de realización de la invención, cuando se fabrica el hardware del aparato (llamado etiquetado), los servidores de seguridad en la fábrica del fabricante pueden generar certificados de hardware 301-303 para todas las variantes de aparatos conocidas a las que se les permite ser ejecutadas en el hardware. Se crea un paquete dedicado 310 de los certificados de hardware 301-303 correspondientes a variantes para un operador/minorista dado de suministro permitido. Dicho paquete 310 puede ser cifrado con una clave pública (PKOx) 315 correspondiente al operador de destino o el minorista de destino. El paquete cifrado, con un identificador de operador/minorista añadido al mismo, se escribe en una memoria del aparato. La memoria puede ser una memoria pasiva que puede ser accesible sin necesidad de apagar el aparato en el almacén del distribuidor. Dicha memoria puede comprender una etiqueta de memoria de radiofrecuencia (RF) incrustada, por ejemplo. El proceso descrito anteriormente puede repetirse para todos los m distribuidores conocidos (operadores o minoristas) de aparatos con este hardware. Con el tiempo la memoria pasiva del aparato puede comprender m diferentes paquetes cifrados en la memoria pasiva.

De acuerdo con un ejemplo de realización de la invención, el aparato puede ser enviado desde la fábrica del fabricante terminando en el almacén del distribuidor. El aparato puede incluso ser re-distribuido entre los almacenes. Cuando el aparato, finalmente, está para ser vendido a un cliente final, el distribuidor, equipado con un escritor de memoria pasiva (por ejemplo, un escritor de etiqueta de memoria de radiofrecuencia (RF)), la clave secreta (SKOx) 325 y una imagen de la variante 331-333 capaz de escribir una imagen de variante 331 a 333 deseada con el certificado de hardware correcto 301-303 en la memoria pasiva del aparato variante. En un ejemplo de realización, el escritor de memoria pasiva puede leer primero el paquete encriptado 320 (etiquetado con el identificador del distribuidor) y descifrar el paquete 320 con la clave secreta (SKOx) 325. A partir de los contenidos descifrados, se selecciona el certificado de hardware 301-303 que corresponde a la imagen de la variante que el distribuidor tiene la intención de escribir en la memoria pasiva del aparato. La imagen 331-333, el certificado de hardware 301-303 y más probablemente es que el certificado de configuración común se puede escribir en la memoria pasiva (por ejemplo, una etiqueta de memoria de radiofrecuencia incrustada (RF)) del aparato. Con dicha información almacenada, el aparato puede arrancar desde la memoria pasiva. Alternativamente, al menos parte de la información puede ser almacenada en otra memoria del aparato para permitir el arranque del aparato. Además, el distribuidor puede borrar todos los otros paquetes de certificado de hardware cifrado de la memoria pasiva después de escribir la imagen de la variante deseada 331-333. Así otros distribuidores no pueden etiquetar de nuevo posteriormente el mismo aparato.

Si la clave secreta (SKOx) 325 es proporcionada por el fabricante de la tarjeta inteligente, los registros de auditoría y controles seguros pueden ser construidos en la tarjeta inteligente para fines de seguridad mejorados. La tarjeta inteligente puede devolver solo un certificado de hardware variante 301-303 para identificador de circuito integrado específico de la aplicación dada (ASIC id) o el identificador público. El certificado de configuración común (CCC) se puede unir a cada imagen de la variante y puede suponerse que combina con la imagen de la variante. Por lo tanto, el certificado de configuración común (CCC) se puede tratar como información pública y, o bien ser escrito previamente con el aparato o acompañar a la imagen de la variante.

De acuerdo con un ejemplo de realización de la invención, los certificados de hardware pueden permitir partes de

variantes estáticas y dinámicas. La parte de variante estática puede comprender todas las posibles variantes del operador y del minorista almacenadas en la memoria del aparato en la fase de fabricación y selectivamente retiradas en una fase posterior cuando se toma la variante en uso. Dicha elección puede permanecer sin cambios después de entrar en uso. La parte de variante dinámica puede cambiar dentro de cierto período de tiempo basada en la parte de variante estática seleccionada. Por ejemplo, un minorista puede ofrecer una variante de ensayo, siendo activa durante un período de tiempo cuando se selecciona cierta parte de variante estática. Dicha variante de prueba puede permitir que usar con seguridad ciertos cambios de variante de software sin tener estar estáticamente en uso. La parte de variante estática seleccionada puede permitir la selección de un cierto conjunto de variantes dinámicas, definiendo las capacidades de las variantes dinámicas y la comprobación de la validez del paquete de certificado de hardware, por ejemplo.

La figura 4 muestra algunos detalles de la determinación de los certificados de hardware y datos de programación de acuerdo con un ejemplo de realización de la invención. Un nuevo aparato es fabricado por un fabricante con un conjunto almacenado de forma segura de las variantes correctas en una memoria pasiva 410 del aparato. Las variantes pueden estar basadas en el minorista, basadas en el operador o basadas en la nube y las variantes pueden ser puestas en uso basadas en las selecciones del usuario.

El nuevo aparato puede comprender varios paquetes dedicados 411-414 de los certificados de hardware almacenados en la memoria pasiva 410 del aparato, por ejemplo. Cada paquete 411-414 puede comprender un identificador para un operador o un minorista, por ejemplo. Sobre la base de dicho identificador, el operador o el minorista puede reconocer el paquete correcto 411-414 a utilizar. Además, el paquete dedicado 411-414 puede comprender certificados permitidos de hardware para el distribuidor (por ejemplo, el operador/minorista) para variantes de aparatos diferentes a ser aprovisionados. Como se describió anteriormente el paquete dedicado 411-414 puede ser cifrado con una clave pública PKOx.

El distribuidor (por ejemplo, el operador/minorista) recibe el aparato para la venta a un usuario final. Dependiendo de la selección del usuario se decide una cierta variante de aparato. El distribuidor puede acceder a la memoria pasiva 420 del aparato distribuidor. La memoria pasiva 410, 420 puede comprender por ejemplo una etiqueta de memoria de radiofrecuencia incrustada (RF). Para acceder a esa memoria 410, 420, el distribuidor puede usar un escritor de radiofrecuencia (escritor RF). El paquete cifrado 421-424 etiquetado con el identificador del distribuidor correcto puede ser leído y descifrado con una clave secreta SKOx apropiada. Sobre la base de la variante de aparato deseada, también se seleccionan unos datos de programación 425 que comprenden la configuración y características del aparato deseado para el usuario final. Los datos de programación 425 se almacenan en la memoria pasiva 420 del aparato. Por lo general, y en esta realización, los datos de programación pueden ser un firmware del aparato, pero ningún software puede implementarse en un mecanismo similar. Además, de escribir el firmware en la memoria pasiva 420, también el certificado de hardware correcto (HWC1) 426 se puede escribir descifrado en la memoria pasiva 420, así como el certificado común de configuración correcto (CCC) 427. Para el caso del "minorista 2", por ejemplo, un firmware 425 deseado del "minorista 2" se almacena en la memoria pasiva 420 junto con el certificado de hardware descifrado HWC1 (que coincide con el firmware 425 del paquete 424) y el certificado de configuración común (CCC) 427.

De acuerdo con un ejemplo de realización de la invención, los paquetes cifrados no utilizados 421-424 pueden ser borrados después del aprovisionamiento de la variante deseada. Además, incluso el paquete de cifrado seleccionado 424 puede ser eliminado después de escribir el firmware 425, el certificado de hardware 426 y el certificado de configuración común 427 en la memoria pasiva 420 del aparato.

En el caso en que paquetes de venta de aparatos no se ponen en uso en un "minorista 2", a continuación, los paquetes pueden ser autorizados a ponerse en uso en un "minorista 1", por ejemplo, sin la entrega de primera vuelta al fabricante. A ambos minoristas se les permite vender los aparatos, por lo que ambos identificadores de minoristas pueden ser almacenados en la memoria pasiva 410 del nuevo aparato.

La figura 5 presenta un diagrama de bloques de ejemplo de un aparato 500 y un dispositivo lector/grabador externo 580 en el que pueden aplicarse diversas realizaciones de la invención. El aparato 500 puede ser un equipo de usuario (UE), dispositivo o aparato de usuario, tal como un terminal móvil u otro dispositivo de comunicación. El dispositivo de lectura/escritura 580 puede ser un dispositivo utilizado por un fabricante de aparatos, el minorista o el operador.

La estructura general del aparato 500 comprende un módulo de interfaz de comunicación 550, un procesador 510 acoplado al módulo de interfaz de comunicación 550, una memoria pasiva 540 y una memoria 520 acoplada al procesador 510. El aparato comprende, además, el software 530 almacenado en la memoria 520 y operable para cargarse en y ser ejecutado en el procesador 510. El software 530 puede comprender uno o más módulos de software y puede estar en la forma de un producto de programa informático. El aparato 500 comprende, además, un controlador de interfaz de usuario 560 acoplado al procesador 510.

El módulo de interfaz de comunicación 550 implementa al menos parte de la radio de datos de usuario descrita en conexión con diversas realizaciones de la invención. El módulo de interfaz de comunicación 550 puede ser, por

ejemplo, un módulo de interfaz de radio, tal como un módulo de radio WLAN, Bluetooth, GSM/GPRS, CDMA, WCDMA, o LTE (Evolución a largo plazo). El módulo de interfaz de comunicación 550 puede estar integrado en el aparato 500 o en un adaptador, tarjeta o similar que puede insertarse en una ranura o puerto adecuado del aparato 500. El módulo de interfaz de comunicación 550 puede soportar tecnología de interfaz de una radio o una pluralidad de tecnologías. La figura 5 muestra una interfaz de comunicación del módulo 550, pero el aparato 500 puede comprender una pluralidad de módulos de interfaz de comunicación 550. El procesador 510 puede ser, por ejemplo, una unidad de procesamiento central (CPU), un microprocesador, un procesador de señal digital (DSP), una unidad de procesamiento de gráficos, o similares. La figura 5 muestra un procesador 510, pero el aparato 500 puede comprender una pluralidad de procesadores.

La memoria 520 puede ser, por ejemplo, una memoria no volátil o una memoria volátil, tal como una memoria de solo lectura (ROM), una memoria programable de solo lectura (PROM), una memoria de solo lectura programable y borrable (EPROM), una memoria de acceso aleatorio (RAM), una memoria flash, un disco de datos, un almacenamiento óptico, un dispositivo de almacenamiento magnético, una tarjeta inteligente, o similares. El aparato 500 puede comprender una pluralidad de memorias. La memoria 520 puede estar construida como una parte del aparato 500 o puede insertarse en una ranura, puerto, o similares del aparato 500 por parte de un usuario. La memoria 520 puede servir para el único propósito de almacenamiento de datos, o puede construirse como una parte de un aparato que sirve para otros fines, tales como el procesamiento de datos.

Una tarjeta de circuito integrado universal (UICC) 570 puede incluirse como una tarjeta inteligente utilizada en el aparato 500. La tarjeta universal de circuito integrado (UICC) 570 asegura la integridad y la seguridad de determinados datos personales. La tarjeta de circuito integrado universal (UICC) 570 puede contener su número de serie único, el número único del usuario móvil internacional (IMSI), la autenticación de seguridad y cifrado de la información, la información temporal relacionada con la red local, una lista de los servicios que el usuario tiene acceso y contraseñas (PIN para su uso habitual y PUK para desbloquear). La tarjeta universal de circuito integrado (UICC) 570 puede comprender, además, varias aplicaciones, por lo que es posible que la misma tarjeta inteligente proporcione acceso a las diferentes redes, y proporcionar almacenamiento de una guía telefónica y otras aplicaciones. El sistema puede utilizar un módulo de seguridad integrado para el almacenamiento y el procesamiento de claves.

El controlador de interfaz de usuario 560 puede comprender circuitos para recibir la entrada de un usuario del aparato 500, por ejemplo, a través de un teclado, interfaz gráfica de usuario mostrada en la pantalla del aparato 500, circuitos de reconocimiento de voz, o un dispositivo accesorio, tal como un auricular, y para proporcionar la salida para el usuario a través de, por ejemplo, una interfaz gráfica de usuario o un altavoz.

La memoria pasiva 540 puede comprender una etiqueta de memoria de radiofrecuencia (RF) integrada. El sistema de etiquetas de memoria de radiofrecuencia (RF) puede proporcionar comunicaciones de alta velocidad de datos a 10-100 Mbit/s entre etiquetas de frecuencia de lector/escritor y dispositivo de radio (RF) que contienen una gran cantidad de memoria (por ejemplo, uno o más Gigabits) que operan a través de un canal de comunicación de datos de muy alta tasa de bits (por ejemplo, ultra amplia banda de radio de impulsos (UWB) a 7,9 GHz). Las realizaciones de ejemplo descritas en este documento pueden diseñarse en la parte superior de un sistema de etiqueta de memoria de radiofrecuencia (RF). El sistema de etiqueta de memoria de radiofrecuencia (RF) puede basarse en comunicación de campo cercano. Los ejemplos de realización utilizan los recursos de memoria del sistema de etiqueta de la memoria de radiofrecuencia (RF) como bloques de memoria no volátiles para proporcionar la capacidad de ejecución en posición para un dispositivo de lectura/escritura 580, tal como el dispositivo distribuidor, para mejorar la variante de aprovisionamiento del aparato con el sistema de etiqueta de memoria de radiofrecuencia (RF).

Un experto aprecia que, además, de los elementos mostrados en la figura 5, el aparato 500 puede comprender otros elementos, tales como micrófonos, pantallas, así como circuitos adicionales, tales como circuitos de entrada/salida (E/S), chips de memoria, circuitos integrados de aplicación específica (ASIC), circuitos de procesamiento para fines específicos tales como circuitos de codificación/decodificación de fuente, circuitos de codificación/decodificación de canal, circuitos de cifrado/descifrado, y similares. Además, el aparato 500 puede comprender una batería desechable o recargable (no mostrada) para alimentar el aparato 500 como alimentación externa si la fuente de alimentación externa no está disponible.

La figura 6 ilustra un ejemplo de realización para un dispositivo de lectura/escritura 600 y una etiqueta de memoria 650 de radiofrecuencia (RF) incrustada en un aparato. El dispositivo de lectura/escritura 600 puede transmitir potencia de radiofrecuencia (RF) y datos al módulo de memoria 650 y el módulo de memoria 650 puede transmitir datos al dispositivo de lectura/escritura 600.

El módulo de memoria 650 puede comprender una memoria 660 para almacenar datos relacionados con el aprovisionamiento, tal como certificados de configuración comunes, firmwares y paquetes cifrados dedicados contienen certificados de hardware, por ejemplo. El módulo de memoria 650 puede comprender, además, un transceptor de potencia de radiofrecuencia 680, un transceptor de datos de RF de alta tasa de bits 690 y un procesador 670. El transceptor de potencia de radiofrecuencia 680 es capaz de recibir la potencia sobre una banda

de ultra alta frecuencia o una comunicación de campo cercano (NFC), por ejemplo. El transceptor de datos de RF 690 de alta tasa de bits puede permitir la comunicación a través de una conexión inalámbrica de corto alcance con el dispositivo 600. El procesador 670 puede ser necesario para controlar las funcionalidades y el procesamiento general en el módulo de memoria 650. Debido a la potencia del transceptor 680, el módulo de memoria 650 puede no necesitar ser alimentado en absoluto por el aparato en el que se encuentra el módulo de memoria.

El dispositivo 600 puede comprender un transceptor de datos de RF 690 de alta velocidad de bits que transmite los paquetes dedicados almacenados y los identificadores de minorista en el dispositivo de lectura/escritura 600 para el almacenamiento y el procesamiento en el dispositivo 600. El ejemplo de dispositivo de lectura/escritura 600 de la figura 6 puede incluir, además, un transceptor de potencia 630 que transmite potencia de radiofrecuencia (RF) al módulo de memoria 650 y un transceptor de datos 640 de radiofrecuencia (RF) de alta tasa de bits para la comunicación. Además, una señal de reloj de onda continua puede ser transmitida al módulo de memoria 650. El transceptor de potencia de radiofrecuencia 630 es capaz de transmitir la potencia a través de una banda de ultra alta frecuencia (UHF) o una comunicación de campo cercano (NFC), por ejemplo. La memoria 610 en el dispositivo de lectura/escritura 600 de ejemplo de la figura 6 puede incluir un programa de sistema operativo. El sistema operativo puede leer/escribir los datos de la memoria 660 transmitidos/recibidos desde el módulo de memoria 650 con el que se está comunicando el dispositivo de lectura/escritura 600.

De acuerdo con un ejemplo de realización de la invención, uno de los dispositivos 600, 650 pueden actuar como una etiqueta de memoria radiofrecuencia (RF) incorporada sin el soporte de procesador como una etiqueta de memoria activa o pasiva. El dispositivo 600, 650 también puede actuar como un dispositivo de pares con el soporte del procesador.

El dispositivo de lectura/escritura 600 puede incluir un módulo de UHF RF conectado a una primera antena de RF para transmitir potencia de RF y pulsos de reloj en un portador de 900 MHz al módulo de memoria 650 para la alimentación y la temporización de los circuitos del módulo de memoria 650. El dispositivo de lectura/escritura 600 puede incluir un módulo de RF de alta tasa de bits 630 conectado a una segunda antena de RF para el intercambio de datos a través de un enlace de impulso de radio de ultra banda ancha (UWB) con el módulo de memoria 650. El dispositivo de lectura/escritura 600 puede incluir un procesador 620 para controlar los componentes en el dispositivo de lectura/escritura 600 y ejecutar instrucciones programadas para llevar a cabo las funciones del dispositivo de lectura/escritura 600.

El módulo de memoria 650 puede incluir un módulo de UHF RF 680 conectado a una primera antena de RF para recibir impulsos de potencia de RF y de reloj sobre un portador de 900 MHz desde el dispositivo de lectura/escritura 600 para la alimentación y la temporización de los circuitos del módulo de memoria 650. El módulo de memoria 650 puede incluir un módulo de RF de alta tasa de bits conectado a una segunda antena de RF para intercambiar datos a través del enlace de radio de impulsos de ultra banda ancha (UWB) con el dispositivo de lectura/escritura 600. El módulo de memoria 650 puede incluir un procesador 670 para controlar los otros componentes en el módulo de memoria 650 de la etiqueta y ejecutar instrucciones programadas para llevar a cabo las funciones del módulo de memoria 650.

La figura 7 muestra un diagrama de flujo que muestra operaciones de acuerdo con un ejemplo de realización de la invención. En la etapa 700, se inicia el método. En la etapa 710, se determina un identificador público para identificar una configuración de un aparato. En la etapa 720 se determina un certificado de configuración común que comprende un identificador de certificado de configuración común para la verificación de los datos de programación. Un certificado de hardware que comprende el identificador público y el identificador de certificado de configuración común para asociar una combinación permitida de la configuración de aparatos y los datos de programación se determina en la etapa 730. Un paquete dedicado de los certificados de hardware correspondientes a las configuraciones de aparatos que se permite siempre se genera en la etapa 740. En la etapa 750, el paquete dedicado de los certificados de hardware utilizando una clave pública está cifrado y el paquete dedicado cifrado de los certificados de hardware con un identificador se almacena en una memoria pasiva del aparato en la etapa 760. El método termina en la etapa 770.

La figura 8 muestra otro diagrama de flujo que muestra operaciones de acuerdo con un ejemplo de realización de la invención. En la etapa 800, se inicia el método. En la etapa 810, un paquete dedicado cifrado de los certificados de hardware de una memoria de un aparato inalámbrico se detecta basándose en un identificador. En la etapa 820, el paquete dedicado cifrado de los certificados de hardware se descifra utilizando una clave privada. Se selecciona el certificado de hardware del paquete dedicado descifrado de los certificados de hardware correspondientes a una configuración deseada del aparato en la etapa 830. La programación de los datos y del certificado de hardware seleccionado se escribe en la memoria pasiva del aparato en la etapa 840 y los certificados de hardware no seleccionados se borran de la memoria pasiva del aparato en la etapa 850. El método termina en la etapa 860.

Diversas realizaciones se han presentado. Debe apreciarse que, en este documento, las palabras comprenden, incluyen y contienen cada una se utilizan como expresiones abiertas sin exclusividad prevista.

La descripción anterior se ha proporcionado a modo de ejemplos de implementaciones y realizaciones de la

invención particulares no limitativas de una descripción completa e instructiva del mejor modo contemplado actualmente por los inventores para llevar a cabo la invención. Sin embargo, es claro para una persona experta en la técnica que la invención no se limita a los detalles de las realizaciones presentadas anteriormente, sino que puede ser implementada en otras realizaciones utilizando medios equivalentes o en diferentes combinaciones de realizaciones sin apartarse de las características de la invención.

Además, algunas de las características de las realizaciones anteriormente descritas de esta invención se pueden utilizar ventajosamente sin el uso correspondiente de otras características. Como tal, la descripción anterior se considerará como meramente ilustrativa de los principios de la presente invención, y no como limitación de la misma. Por lo tanto, el alcance de la invención solamente está limitado por las reivindicaciones de patente adjuntas.

REIVINDICACIONES

1. Un método que comprende:

determinar un identificador público para identificar una configuración de un aparato;
determinar un certificado de configuración común que comprende un identificador de certificado de configuración común para la verificación de los datos de programación;
determinar un certificado de hardware que comprende el identificador público y el identificador de certificado de configuración común para asociar una combinación permitida de la configuración de aparatos y los datos de programación;
generar un paquete dedicado de los certificados de hardware correspondientes a las configuraciones de aparatos permitidas para ser proporcionadas;
cifrar el paquete dedicado de los certificados de hardware utilizando una clave pública; y
almacenar el paquete dedicado cifrado de los certificados de hardware con un identificador en una memoria pasiva del aparato.

2. Un método que comprende:

detectar un paquete dedicado cifrado de los certificados de hardware de una memoria inalámbrica de un aparato basado en un identificador;
descifrar el paquete dedicado cifrado de los certificados de hardware utilizando una clave privada;
seleccionar el certificado de hardware del paquete dedicado descifrado de los certificados de hardware correspondientes a una configuración deseada del aparato;
escribir datos de programación y el certificado de hardware seleccionado en la memoria pasiva del aparato; y
borrar de la memoria pasiva del aparato certificados de hardware no seleccionados.

3. Un método según la reivindicación 2, que comprende, además:

firmar los datos de programación con una clave común que se utiliza para todas las combinaciones permitidas de la configuración del aparato y los datos de programación.

4. Un método según cualquier reivindicación anterior 2 a 3, en el que los datos de programación se seleccionan del grupo que comprende:

firmware;
software del sistema operativo;
datos de configuración;
software de aplicación;
contenidos multimedia; y
controladores.

5. Un método según cualquier reivindicación anterior 2 a 4, que comprende, además:

detectar un identificador estático para identificar una configuración estática del aparato.

6. Un método según cualquier reivindicación anterior 2 a 5, que comprende, además:

detectar un identificador dinámico para la identificación de una configuración dinámica del aparato.

7. Un método según la reivindicación 6, en el que la configuración dinámica del aparato está activa durante un período de tiempo fijo.

8. Un método según cualquier reivindicación anterior 2 a 7, que comprende, además:

transmitir de forma inalámbrica los datos de programación y el certificado de hardware seleccionado a la memoria pasiva del aparato.

9. Un método según cualquier reivindicación anterior 2 a 8, en el que la memoria pasiva del aparato comprende una etiqueta de memoria de radiofrecuencia (RF) incrustada que es accesible de forma inalámbrica y que está alimentada desde un aparato externo.

10. Un dispositivo que comprende:

una interfaz de comunicaciones inalámbrica de corto alcance configurada para comunicarse con un aparato;
al menos un procesador; y
al menos una memoria que incluye código de programa de ordenador, estando configurada la al menos una

memoria y el código de programa de ordenador para, con el al menos un procesador, hacer que el dispositivo al menos:

determine un identificador público para identificar una configuración del aparato;
determine un certificado de configuración común que comprende un identificador de certificado de configuración común para la verificación de los datos de programación;
determine un certificado de hardware que comprende el identificador público y el identificador de certificado de configuración común para asociar una combinación permitida de la configuración de aparatos y los datos de programación;
genere un paquete dedicado de los certificados de hardware correspondientes a las configuraciones de aparatos permitidas para ser proporcionadas;
cifrar el paquete dedicado de los certificados de hardware utilizando una clave pública; y
almacenar el paquete dedicado cifrado de los certificados de hardware con un identificador en una memoria pasiva del aparato.

11. Un dispositivo que comprende:

una interfaz de comunicaciones inalámbricas de corto alcance configurada para comunicarse con un aparato;
al menos un procesador; y
al menos una memoria que incluye código de programa de ordenador, estando la al menos una memoria y el código de programa de ordenador configurados para, con el al menos un procesador, hacer que el dispositivo al menos:

detecte un paquete dedicado cifrado de los certificados de hardware de una memoria inalámbrica del aparato basado en un identificador;
descifre el paquete dedicado cifrado de los certificados de hardware utilizando una clave privada;
seleccione el certificado de hardware del paquete dedicado descifrado de los certificados de hardware correspondientes a una configuración deseada del aparato;
escriba datos de programación y el certificado de hardware seleccionado en la memoria pasiva del aparato; y
borre de la memoria pasiva del aparato certificados de hardware no seleccionados.

12. Un aparato según la reivindicación 11, que comprende, además:

medios para realizar un método según cualquiera de las reivindicaciones 3 a 9.

13. Un programa de ordenador incorporado en un medio legible por ordenador que comprende un código de programa ejecutable por ordenador que, cuando es ejecutado por al menos un procesador de un aparato, hace que el aparato realice:

la determinación de un identificador público para identificar una configuración de un aparato;
la determinación de un certificado de configuración común que comprende un identificador de certificado de configuración común para la verificación de los datos de programación;
la determinación de un certificado de hardware que comprende el identificador público y el identificador de certificado de configuración común para asociar una combinación permitida de la configuración de aparatos y los datos de programación;
la generación de un paquete específico de los certificados de hardware correspondientes a las configuraciones de aparatos permitidas para ser proporcionadas;
cifrar el paquete dedicado de los certificados de hardware utilizando una clave pública; y
almacenar el paquete dedicado cifrado de los certificados de hardware con un identificador en una memoria pasiva del aparato.

14. Un programa de ordenador incorporado en un medio legible por ordenador que comprende un código de programa ejecutable por ordenador que cuando es ejecutado por al menos un procesador de un aparato, hace que el aparato realice:

la detección de un paquete dedicado cifrado de los certificados de hardware de una memoria inalámbrica de un aparato basado en un identificador;
el descifrado del paquete dedicado cifrado de los certificados de hardware utilizando una clave privada;
la selección del certificado de hardware del paquete dedicado descifrado de los certificados de hardware correspondientes a una configuración deseada del aparato;
la escritura de datos de programación y el certificado de hardware seleccionado en la memoria pasiva del aparato; y
el borrado de la memoria pasiva del aparato de los certificados de hardware no seleccionados.

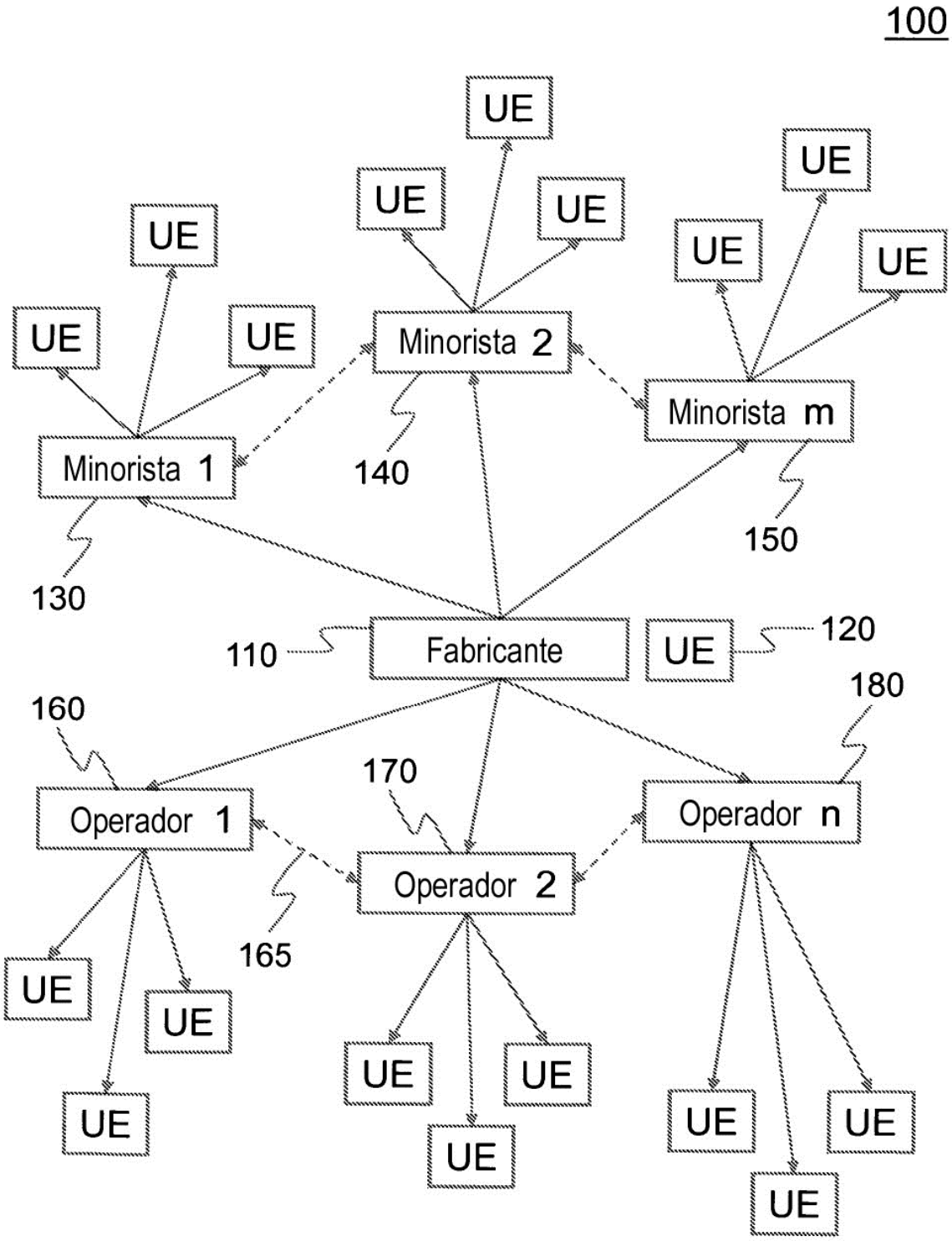
100
UE
UE
UE
UE
UE
UE
UE
UE
UE
UE
Minorista 2
Minorista m
Minorista 1
140
150
130
110
Fabricante
UE
120
180
160
170
Operador 1
Operador n
Operador 2
165
UE
UE
UE
UE
UE
UE
UE
UE
UE

Fig. 1

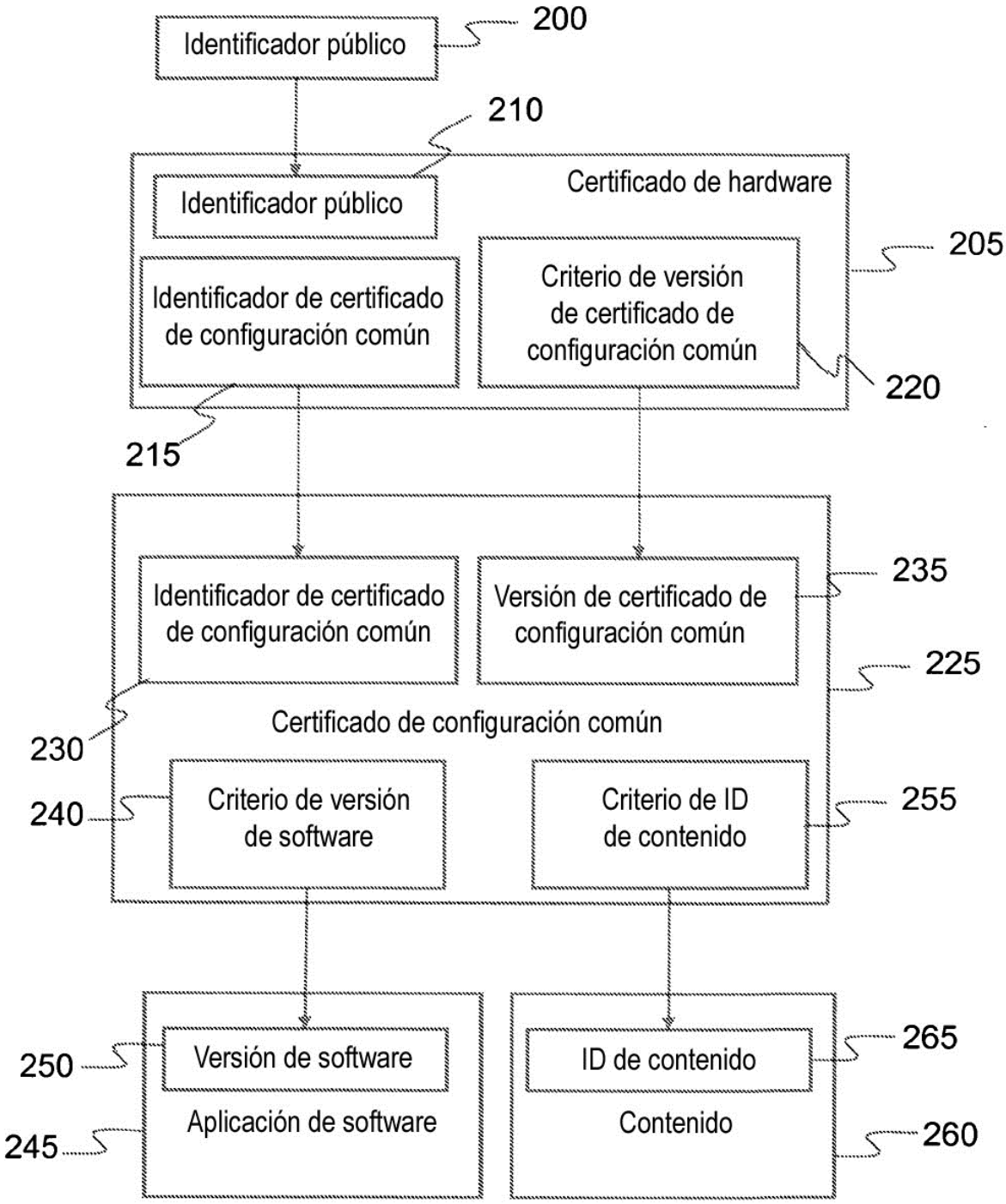
Identificador público
200
210
Identificador público
Certificado de hardware
205
Identificador de certificado de configuración común
Criterio de versión de certificado de configuración común
220
215
Identificador de certificado de configuración común
Versión de certificado de configuración común
235
225
Certificado de configuración común
230
240
Criterio de versión de software
Criterio de ID de contenido
255
250
Versión de software
Aplicación de software
245
ID de contenido
Contenido
265
260

Fig. 2

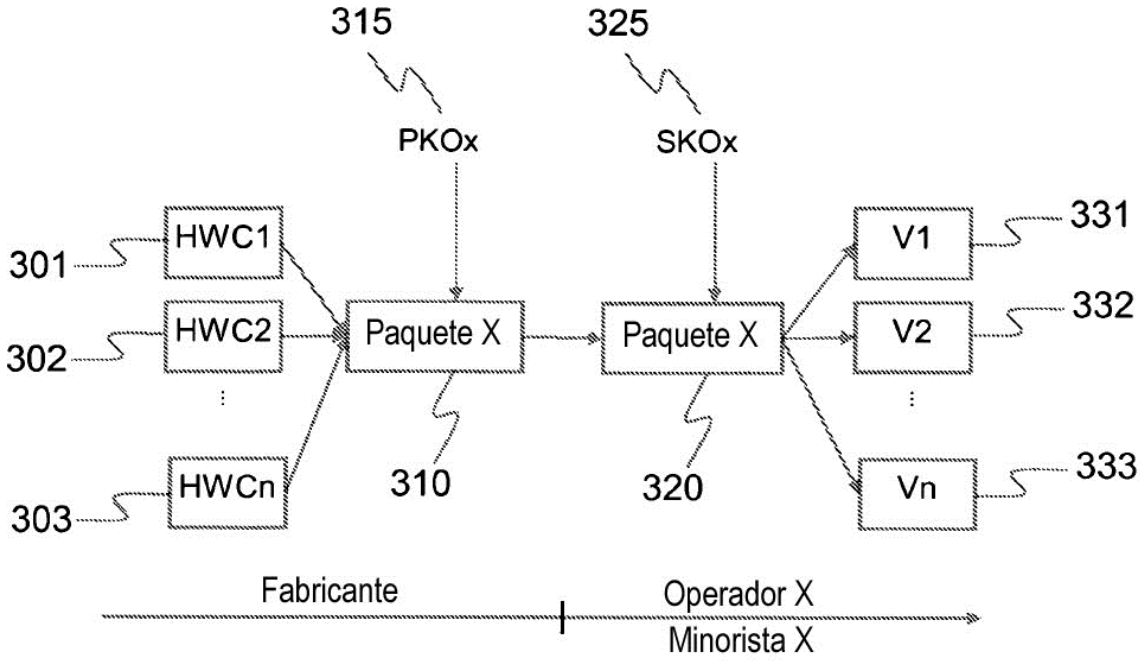
315
325
PKOx
SKOx
301
HWC1
302
HWC2
303
HWCn
Paquete X
310
Paquete X
320
V1
V2
Vn
331
332
333
Fabricante
Operador X
Minorista X

Fig. 3

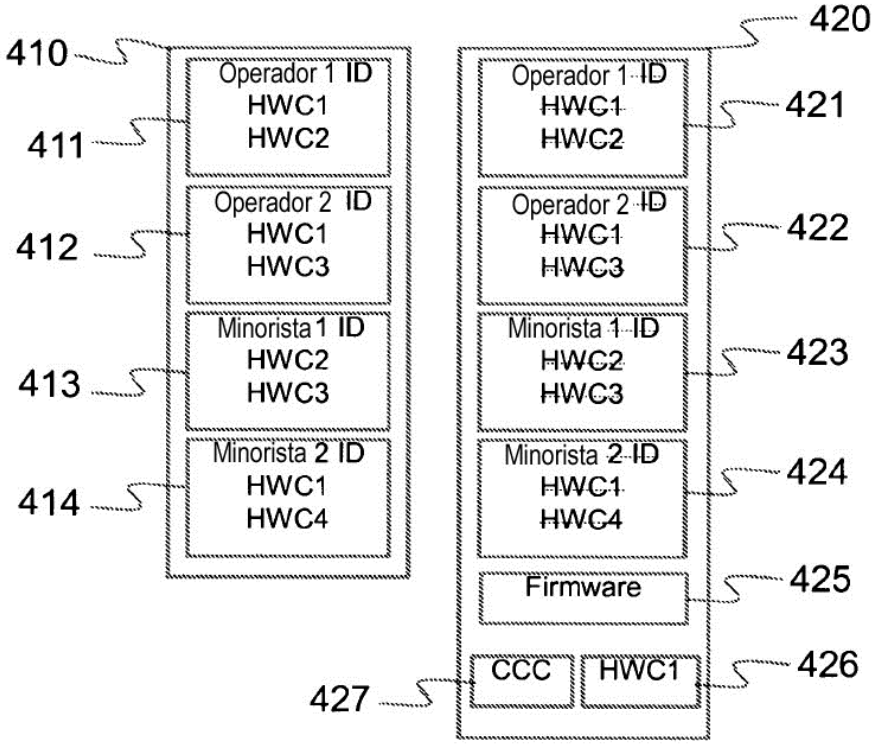
410
411
412
413
414
Operador 1 ID
HWC1
HWC2
Operador 2 ID
HWC1
HWC3
Minorista 1 ID
HWC2
HWC3
Minorista 2 ID
HWC1
HWC4
420
421
422
423
424
425
426
427
Operador 1 ID
HWC1
HWC2
Operador 2 ID
HWC1
HWC3
Minorista 1 ID
HWC2
HWC3
Minorista 2 ID
HWC1
HWC4
Firmware
CCC
HWC1

Fig. 4

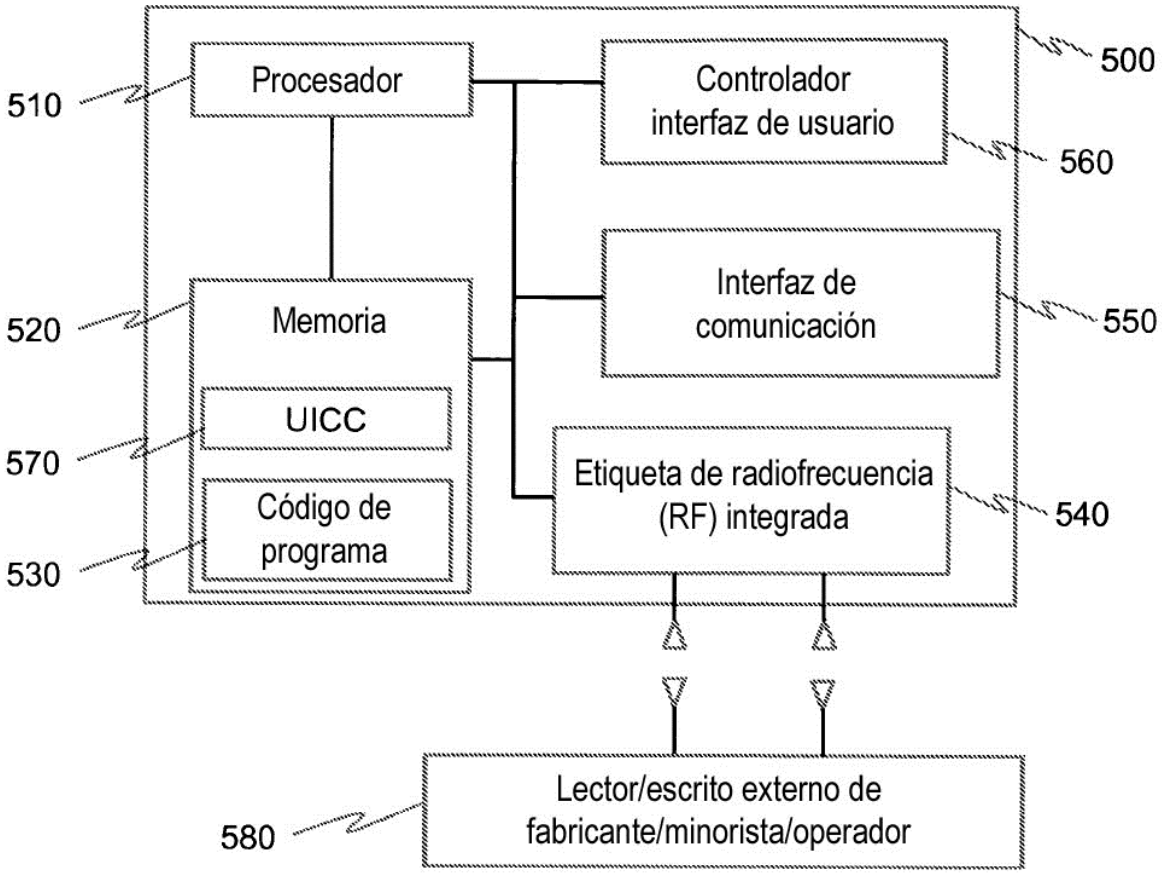
500
510
Procesador
Controlador interfaz de usuario
560
520
Memoria
Interfaz de comunicación
550
UICC
570
Etiqueta de radiofrecuencia (RF) integrada
540
Código de programa
530
580
Lector/escrito externo de fabricante/minorista/operador

Fig. 5

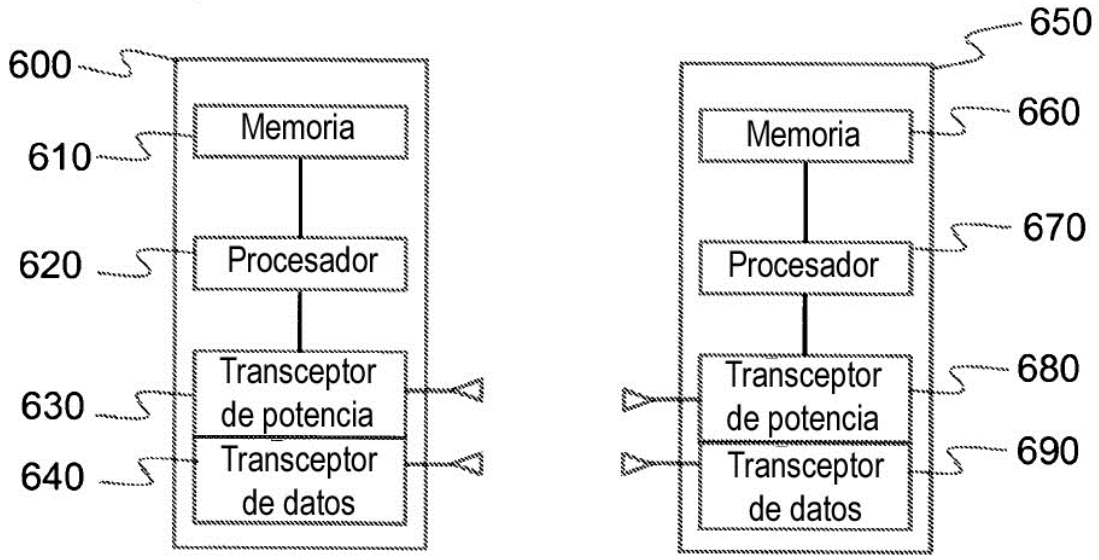
600
610
Memoria
620
Procesador
630
Transceptor de potencia
640
Transceptor de datos
650
660
Memoria
670
Procesador
680
Transceptor de potencia
690
Transceptor de datos

Fig. 6

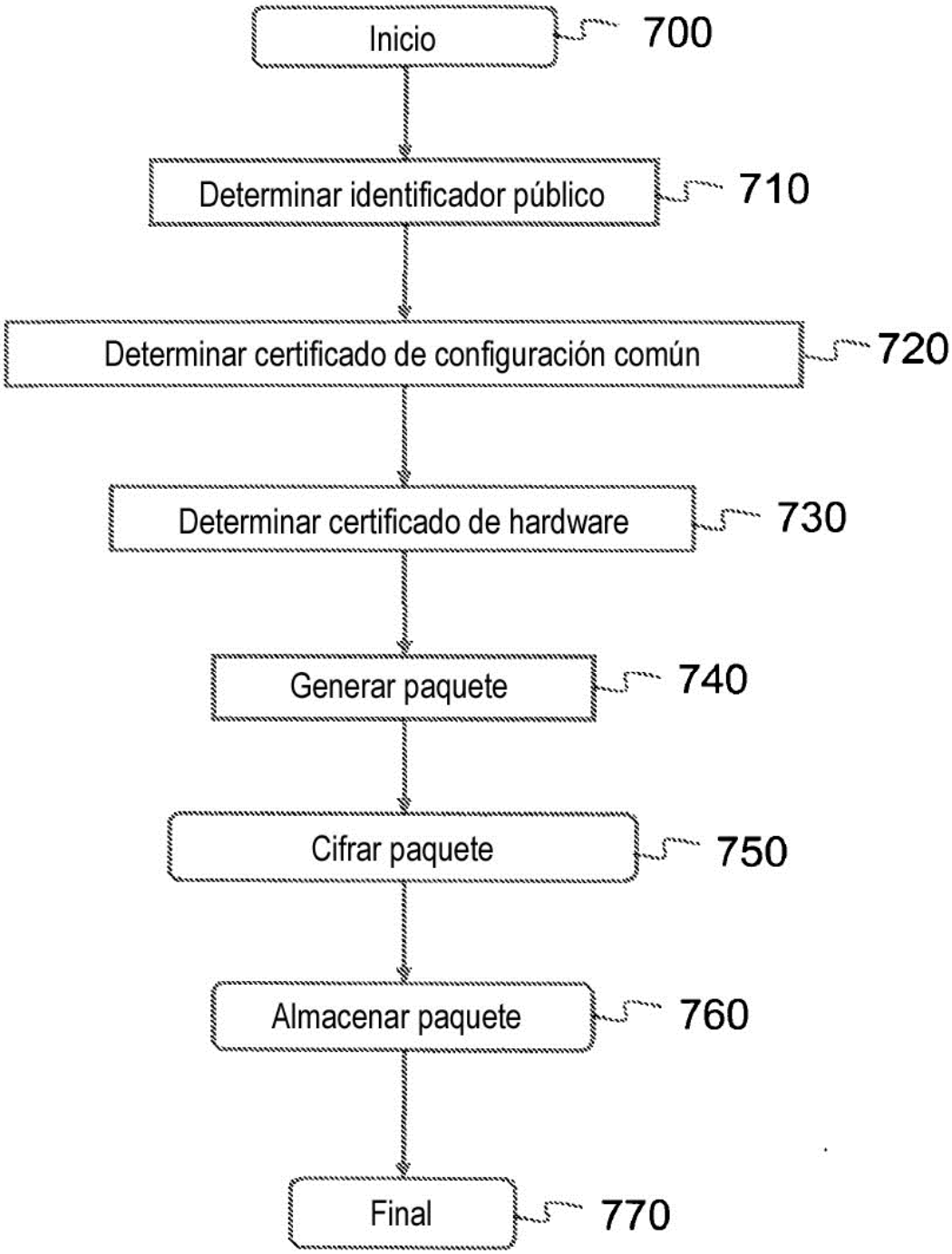
Inicio
700
Determinar identificador público
710
Determinar certificado de configuración común
720
Determinar certificado de hardware
730
Generar paquete
740
Cifrar paquete
750
Almacenar paquete
760
Final
770

Fig. 7

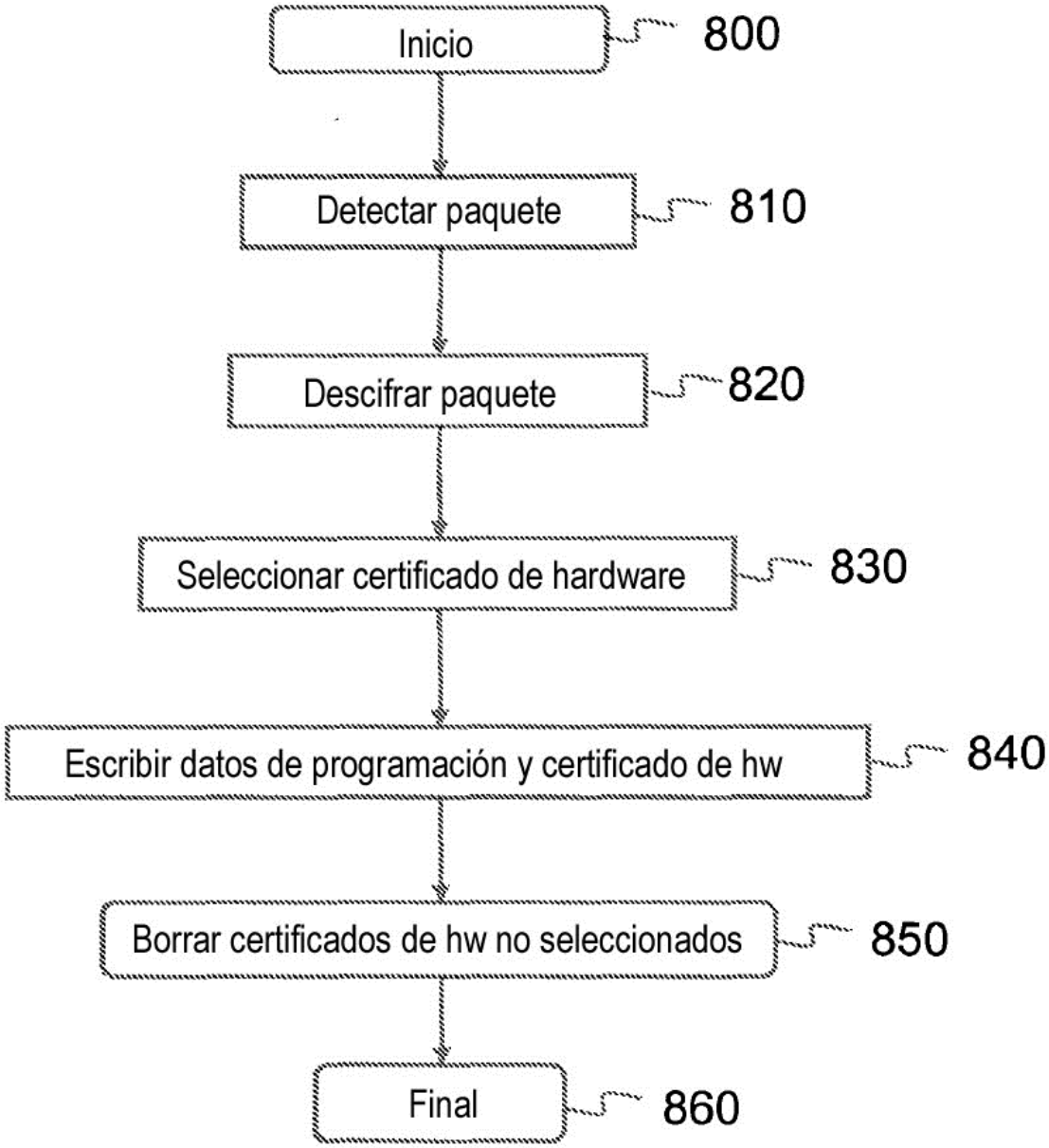
Inicio
800
Detectar paquete
810
Descifrar paquete
820
Seleccionar certificado de hardware
830
Escribir datos de programación y certificado de hw
840
Borrar certificados de hw no seleccionados
850
Final
860

Fig. 8