(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 782 359**

(51) Int. CI.:

G06F 21/10 (2013.01)
G06F 21/60 (2013.01)
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
G06F 8/61 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **12.08.2011 PCT/IT2011/000298**

(87) Fecha y número de publicación internacional: **21.02.2013 WO13024497**

(96) Fecha de presentación y número de la solicitud europea: **12.08.2011 E 11770884 (2)**

(97) Fecha y número de publicación de la concesión europea: **08.01.2020 EP 2742453**

(54) Título: **Procedimiento y sistema para la transmisión protegida de archivos**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.09.2020

(73) Titular/es:

ABB SCHWEIZ AG (100.0%)
Brown Boveri Strasse 6
5400 Baden, CH

(72) Inventor/es:

CHECCUCCI, ALESSANDRO;
TAZZARI, DAVIDE y
VERNIA, FILIPPO

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Procedimiento y sistema para la transmisión protegida de archivos

Campo técnico

La presente invención se refiere a un procedimiento y un sistema para gestionar la transmisión de programas informáticos protegidos, por ejemplo, para programar y/o actualizar dispositivos remotos.

Técnica anterior

La tecnología actual permite la programación y actualización de programa informático residente en dispositivos eléctricos y electrónicos remotos. El programa informático de aplicación y los sistemas operativos de los ordenadores domésticos comunes, PC y ordenadores portátiles, también se actualizan de manera constante y periódica, ya sea a pedido del usuario o de forma automática. De manera similar, es una práctica común actualizar a través del microprograma de Internet para la gestión de una amplia gama de dispositivos electrónicos tales como reproductores de CD y DVD, PlayStations, enrutadores de conexión a Internet, etc. Esto ofrece a los usuarios ventajas obvias.

La posibilidad de actualizar dispositivos remotos también es una ventaja para los fabricantes de los dispositivos, por ejemplo, pueden distribuir los dispositivos equipados con programas informáticos o microprograma en una versión reducida e ingresar al mercado en un plazo mucho más rápido que el que normalmente se requiere para desarrollar y probar un programa informático completo. El usuario final puede adquirir, de forma gratuita o mediante pago, las versiones actualizadas y más avanzadas del programa informático o microprograma. El usuario final también puede estar seguro de que el producto adquirido se mantiene y que cualquier problema de programa informático futuro puede abordarse y resolverse. Además, el fabricante tendrá la ventaja de que puede corregir defectos de programa informático y/o microprograma que están inevitablemente presentes en las primeras versiones comercializadas.

El desarrollo de la tecnología y la conectividad entre equipos electrónicos, procesadores, servidores de red, etc., ha ampliado considerablemente la posibilidad de conectar cualquier dispositivo a un sistema, por ejemplo, un servidor de la empresa, para descargar programa informático nuevo o actualizado. La actualización en línea está disponible en un número creciente de situaciones, tanto gratuitas como de pago, por ejemplo, en forma de suscripción anual. Los sistemas operativos para ordenadores personales, programas antivirus y programa informático de aplicación para ordenadores son algunos de los ejemplos más comunes.

En el sector industrial y de producción, pueden ocurrir situaciones en las que una empresa requiere un suministro externo para compensar las deficiencias o límites internos, por ejemplo, una capacidad de producción limitada o simplemente una política de organización de manera que algunas partes o equipos son producidos por empresas externas. En todos estos casos es necesario intercambiar información confidencial (diagramas de cableado, planos de montaje, planos mecánicos, microprograma, etc.). Las herramientas legales, tales como los acuerdos de confidencialidad (NDA) no siempre brindan una protección adecuada de los conocimientos de propiedad de la empresa. Además, si la producción se subcontrata a terceros, siempre existe el riesgo de una sobreproducción destinada al mercado paralelo con las consiguientes pérdidas económicas, que pueden ser considerables, para la empresa propietaria de los conocimientos y la propiedad intelectual.

El documento US 2009/0202069 divulga un sistema para actualizaciones seguras de microprograma donde las imágenes de microprograma se cifran antes de cargarlas en un dispositivo, que tiene claves para autenticar el microprograma y descifrarlo. Sin embargo, este sistema requiere un manejo complejo de las claves almacenadas en el dispositivo.

Las Figuras 1 y 2 muestran esquemáticamente dos posibles sistemas de conexión de un dispositivo remoto a un servidor de una empresa de fabricación, por ejemplo, para programar o actualizar los archivos de dicho dispositivo.

Más específicamente, la Figura 1 muestra un diagrama funcional de un sistema en el que un dispositivo genérico 1, por ejemplo un dispositivo electrónico o equipo electrónico, con programa informático o microprograma incorporado, se conecta a través de Internet I a un servidor de la empresa 3 para descargar de forma autónoma una actualización residente en el servidor de la empresa 3. Este último está conectado a una base de datos que contiene datos sensibles indicados por 5 y a un archivo de microprograma o programa informático indicado por 7.

En lugar de una conexión directa del dispositivo 1 al servidor 3 a través de Internet I, puede proporcionarse una conexión indirecta a través de un ordenador local, por ejemplo, una PC o un ordenador portátil al que está conectado el dispositivo 1 y que a su vez está conectado a Internet I. En este caso, es el ordenador local el que establece la conexión y descarga el programa informático o microprograma para luego actualizar el dispositivo 1. En este caso, el ordenador puede conectarse físicamente (por medio de una conexión cableada o inalámbrica o de otra manera) al dispositivo que se va a actualizar, o la conexión puede proporcionarse manualmente, es decir, el programa informático/microprograma actualizado puede descargarse a través del ordenador desde Internet I y luego pase al

dispositivo para actualizarse mediante un soporte de memoria, por ejemplo, una memoria flash, un DVD, un CD u otro soporte.

Un sistema diseñado como en la Figura 1 no tiene protección y un ataque al servidor de la empresa 3 pondría en peligro los datos sensibles.

Para evitar esta circunstancia, generalmente se proporciona una arquitectura del tipo ilustrado esquemáticamente en la Figura 2: el dispositivo 1 se conecta a un servidor público (servidor web) 11 que tiene acceso a una base de datos que contiene datos no sensibles, indicados genéricamente por 13. El servidor de la empresa, nuevamente indicado por 3, está conectado a la base de datos 5 que contiene los datos sensibles y al archivo de programa informático o microprograma 7, que debe protegerse del exterior. Esta protección se proporciona por un cortafuegos 15 que impide el acceso directo al servidor de la empresa 3 por un dispositivo externo, ya sea un dispositivo genérico en el campo que requiere una actualización o descarga de programa informático/microprograma o si es un ordenador a su vez conectado o conectable al dispositivo que se actualizará.

De esta manera, el dispositivo o el usuario externo tiene acceso solo al área indicada como DMZ (en la jerga Zona Desmilitarizada) a través de la cual puede acceder, por ejemplo, a una serie de servicios de la empresa, pero no puede acceder de manera incontrolada al área que contiene los datos sensibles, el programa informático/microprograma y, en general, los conocimientos de la empresa propietaria del servidor.

Existen otras técnicas para la protección de datos sensibles en una situación en la que un usuario externo puede solicitar acceso, a través de Internet u otra conexión no protegida, a un servidor de la empresa, por ejemplo, la tecnología NAT (traducción de direcciones de red).

Para proteger el contenido de la información del microprograma o programa informático en tránsito a través de un canal no protegido, por ejemplo a través de Internet o por correo electrónico, el microprograma o el programa informático se cifra para que un tercero no pueda reconocerlo. Actualmente hay una gran cantidad de técnicas de cifrado de varios tipos. Todas las técnicas de cifrado se basan en el uso de al menos una clave de codificación o cifrado, llamada clave maestra, o una pluralidad de dichas claves, que permanecen secretas y típicamente poseen las partes que, dentro de un sistema de gestión de información, son responsables de cifrar y descifrar el programa informático o microprograma. El algoritmo de cifrado se basa en la dificultad intrínseca de recuperar la información original (el código del programa antes del cifrado) a partir de la información cifrada sin conocer la clave o claves de cifrado.

En el caso de dispositivos en el campo a actualizar, la clave o claves de cifrado deben residir en el gestor de arranque, es decir, en el programa responsable de iniciar las funciones del dispositivo cada vez que dicho dispositivo se enciende. Esto es necesario ya que el gestor de arranque es el único programa capaz de actualizar el dispositivo y, por lo tanto, requiere el conocimiento de la clave o claves de cifrado para descifrar el programa informático o microprograma actualizado que se descarga o, en cualquier caso, se suministra al dispositivo.

En los sistemas tradicionales hay varios puntos vulnerables que pueden constituir agujeros de seguridad en los sistemas de transmisión de códigos cifrados o programa informático/microprograma:

- los códigos fuente, es decir, el programa informático o microprograma no cifrado, están disponibles también para personas no autorizadas y, en cualquier caso, la persona que escribe el código conoce las claves de cifrado. El personal inescrupuloso podría robar esta información y usarla para sí mismos o transmitirla a sujetos no autorizados;
- el gestor de arranque en formato ejecutable (código binario) está necesariamente escrito en texto plano porque de cualquier otra manera no sería funcional para el microcontrolador que tiene que usarlo. Este código no cifrado también está disponible fuera de la empresa propietaria del programa informático que se va a proteger, por ejemplo, puede suministrarse a empresas de terceros a las que se externaliza la producción de los dispositivos, o puede estar presente en sitios de producción no seguros, por ejemplo, deslocalizado con respecto a la sede de la empresa propietaria de los conocimientos;
- el código binario del programa de descifrado necesario para reprogramar integralmente el dispositivo con el código en texto plano. Normalmente, esta información la posee solo la empresa propietaria de los conocimientos y está destinada únicamente para uso interno. El suministro de esta información a los técnicos para su intervención en el campo, por ejemplo en las instalaciones de un cliente, expondría a la empresa al riesgo de pérdida de información confidencial.

Para reducir el riesgo derivado del tercer factor mencionado anteriormente, existe un programa informático que proporciona un programa de aplicación de conversión que es difícil de descifrar. Actualmente, las otras dos fuentes de riesgo actualmente no pueden neutralizarse efectivamente.

En resumen, en el escenario brevemente descrito anteriormente, pueden ocurrir múltiples problemas, que incluyen:

- garantizar que el dispositivo que se va a actualizar es un dispositivo autorizado para obtener la actualización, por ejemplo, un dispositivo por el cual la tarifa de actualización se ha pagado debidamente, o que es un dispositivo original del fabricante que pone a disposición sus actualizaciones de programa informático;
- garantizar la correspondencia correcta entre el programa informático/microprograma descargado y el dispositivo en el que está instalado;
- evitar la intercepción de la transmisión de un programa informático o microprograma de actualización por un tercero no autorizado, que podría hacer un uso fraudulento de él;
- evitar que se instale una actualización no autorizada en un dispositivo;
- permitir al usuario final una actualización eficiente de su programa informático/microprograma, al mismo tiempo que protege la información confidencial del fabricante;
- garantizar que un tercer fabricante, a quien se le ha subcontratado la producción de ciertos artículos, produzca el número y tipo de artículos permitidos y no otros;
- seguir los productos distribuidos con fines de mantenimiento o servicio en general.

Sumario de la invención

La invención propone un nuevo procedimiento y un nuevo sistema que permiten que al menos algunos de los problemas mencionados anteriormente, relacionados con la seguridad en la gestión de los conocimientos y, en particular, en la transferencia de programa informático y datos accesorios, se superen total o parcialmente. Por programa informático, cualquier código, en formato fuente o formato ejecutable, incluido el microprograma, los sistemas operativos, el programa informático de aplicación, etc., se entiende por datos accesorios, cualquier tipo de datos vitales para la aplicación, tales como tablas, imágenes, parámetros de configuración, archivos de sonido, etc..

En la siguiente descripción y en las reivindicaciones adjuntas, el programa informático y/o microprograma se define como un programa genérico, también llamado código, que consiste en una secuencia de instrucciones que debe ser ejecutada, compilada, interpretada o traducida de manera directa o apropiada, por un microcontrolador, además de cualquier dato accesorio, como se definió anteriormente, si está previsto. Los términos programa informático y microprograma, aunque se usan alternativamente o en combinación, definen un programa o parte de un programa, que puede consistir o formar parte de un gestor de arranque, un sistema operativo, un programa informático de aplicación genérico u otro. Por microcontrolador se entiende genéricamente un circuito electrónico, capaz de ejecutar un programa. Por sitio de producción se entiende genéricamente un lugar, usado para una o más de las siguientes operaciones: fabricación, programación, montaje, mantenimiento, reconversión, actualización, reacondicionamiento o cualquier otra operación de soporte físico o programa informático en una pieza de un equipo genérico que contiene al menos una parte electrónica. Por empresa propietaria de los conocimientos se entiende un tema físico o jurídico, que posee información confidencial, en particular en forma de programa informático o microprograma.

Sustancialmente de acuerdo con una realización, para resolver total o parcialmente los problemas de seguridad relacionados con la transferencia de programa informático propietario de una empresa a uno o más dispositivos, la invención proporciona un sistema para la gestión de dispositivos electrónicos programables, que comprende:

- una pluralidad de dispositivos electrónicos, cada uno identificado por al menos un parámetro de identificación única y que contiene al menos una clave de cifrado;
- al menos un sitio protegido en el que reside una base de datos protegida, en el que para cada dispositivo electrónico se almacenan el parámetro de identificación única respectivo y la clave de cifrado respectiva;
- un servidor programado: para recibir de uno de dichos dispositivos una solicitud para transmitir un programa informático; y para generar una versión cifrada de dicho programa informático, mediante el uso de la clave de cifrado asociada en dicha base de datos con el parámetro de identificación única del dispositivo que ha solicitado dicha transmisión de programa informático.

El parámetro de identificación única puede atribuirse al dispositivo en la fase de producción o en la fase de programación inicial. Por ejemplo, el parámetro de identificación única puede ser dado por uno o más datos insertados en el chip del microcontrolador incorporado en el dispositivo y programado por el fabricante del chip, o el parámetro de identificación única puede insertarse por la empresa propietaria de los conocimientos a proteger.

Análogamente, la clave de cifrado puede almacenarse por el fabricante del microcontrolador instalado en el dispositivo o puede atribuirse por la empresa propietaria del programa informático o los conocimientos técnicos que se protegerán.

Como se verá claramente a partir de la descripción detallada de las realizaciones de la invención, con un sistema de este tipo es posible programar y/o actualizar varios dispositivos que protegen el programa informático, que se transfiere desde el área o sitio protegido al dispositivo en versión cifrada mediante una clave de cifrado que no se transfiere junto con el programa informático y que en general nunca se transmite de un punto a otro del sistema. Es imposible para una persona mal intencionada apropiarse de la clave de cifrado y esto hace que sea prácticamente imposible descifrar y, por lo tanto, usar ilegalmente el programa informático.

En realizaciones ventajosas, el servidor está programado para almacenar información relativa a las transmisiones de programa informático a los dispositivos, y para subordinar la transmisión de un programa informático solicitado por uno de dichos dispositivos a al menos una condición definida por dicha información. Por ejemplo, el servidor puede programarse para evitar una segunda transmisión de un programa informático a un dispositivo al que dicho programa informático ya se ha enviado una vez. Para dicho propósito, para cada transmisión de programa informático, es suficiente que se almacene información que permita al servidor saber qué dispositivo (identificado por su parámetro de identificación única) ha recibido qué programa informático o qué versión de programa informático. Esto hace que el uso de dispositivos clonados sea imposible. De hecho, si existen dos dispositivos clonados, caracterizados por el mismo parámetro de identificación única, solo uno de ellos puede actualizarse.

En algunas realizaciones, el sistema puede comprender uno o más sitios de producción, diferentes del sitio protegido y, si es necesario, también ubicado a una distancia de este último. En el sitio de producción o en cada sitio de producción, los dispositivos se fabrican y/o ensamblan y/o programan. El sitio de producción o cada sitio de producción pueden no estar bajo el control de la empresa propietaria de los conocimientos técnicos a proteger. En el sitio de producción o en cada uno de ellos, puede proporcionarse un programador para recibir un programa informático del servidor del sitio protegido y programar los dispositivos con el programa informático transferido desde el sitio protegido.

En algunas realizaciones, se proporciona un generador de programas en el sitio protegido para generar un programa informático asociado con el parámetro de identificación única del dispositivo programable respectivo que solicita la instalación del programa informático. El generador de programas también combina con el programa informático una clave de cifrado correspondiente a dicho parámetro de identificación única del dispositivo que ha solicitado el programa informático o para el cual está destinado el programa informático. El programa informático se cifra con dicha clave de cifrado y se envía al dispositivo identificado por el parámetro de identificación única.

El servidor puede programarse adecuadamente para: recibir una solicitud de un programa informático por parte de uno de dichos dispositivos, dicha solicitud comprende al menos el parámetro de identificación única del dispositivo solicitante; verificar si el parámetro de identificación única del dispositivo que ha solicitado el programa informático está contenido en la base de datos protegida; si el parámetro de identificación única del dispositivo solicitante está contenido en la base de datos protegida, verifique si el dispositivo solicitante cumple al menos una condición de habilitación de actualización; si se cumple dicha condición, enviar al dispositivo solicitante una versión del programa informático solicitado, cifrada con la clave de cifrado asociada con el parámetro de identificación única del dispositivo solicitante. La solicitud puede enviarse de manera automática o por un operador. La solicitud puede reenviarse, por ejemplo, a través de un canal no protegido, a través de Internet o de otra manera. En algunas realizaciones, la solicitud puede ejecutarse manualmente, por ejemplo, por un operador que físicamente recibe o descarga en una memoria compatible con el programa informático y luego se ocupa de la programación. La condición de habilitación de actualización puede correlacionarse, por ejemplo, con la existencia de un contrato de mantenimiento o actualización, o la existencia de un contrato de garantía. En algunas realizaciones, el dispositivo puede recibir el programa informático solicitado solo si el servidor reconoce dicho dispositivo como habilitado. En algunas realizaciones, la condición de habilitación de actualización puede correlacionarse con solicitudes de actualización anteriores. Por ejemplo, la condición de habilitación puede cumplirse cuando el dispositivo solicitante no ha solicitado previamente la misma actualización y no se satisface si el dispositivo solicitante ya ha solicitado previamente la misma actualización. En casos más complejos, la condición de habilitación de actualización puede cumplirse cuando el dispositivo solicitante ha realizado previamente todas las actualizaciones antes de la solicitada. En general, una condición de habilitación de actualización correlacionada con solicitudes de actualización anteriores puede reducir o evitar la posibilidad de actualizar dispositivos clonados ilegalmente.

En algunas realizaciones, el servidor en el área protegida está programado para suministrar, a cada uno de dichos dispositivos, un gestor de arranque, y en particular un gestor de arranque asociado con una clave de cifrado y/o con un parámetro de identificación única del dispositivo, o ambos.

De acuerdo con una realización diferente, la invención se refiere a un procedimiento para instalar un programa informático en una pluralidad de dispositivos electrónicos, que comprende las etapas de:

- asociar con cada dispositivo electrónico al menos un parámetro de identificación única y al menos una clave de cifrado;
- almacenar, en una base de datos protegida, el parámetro de identificación única respectivo y la clave de cifrado respectiva para cada dispositivo;
- cifrar un programa informático que se instalará en uno de dichos dispositivos con la clave de cifrado de dicho dispositivo;
- transferir dicho programa informático cifrado a dicho dispositivo;
- instalar el programa informático en dicho dispositivo.

En algunas realizaciones, el procedimiento puede comprender las etapas de:

- generar una solicitud de programa informático por uno de dichos dispositivos, comprendiendo dicha solicitud al menos el parámetro de identificación única del dispositivo solicitante;

- comprobar que el parámetro de identificación única del dispositivo que solicita dicho programa informático está contenido en dicha base de datos protegida;
- si el parámetro de identificación única del dispositivo solicitante está contenido en la base de datos protegida, verificar al menos una condición relativa a solicitudes de actualización anteriores por parte del dispositivo solicitante;
- si se cumple dicha condición, se envía a dicho dispositivo solicitante una versión del programa informático solicitado, cifrada con la clave de cifrado asociada con el parámetro de identificación única del dispositivo solicitante.

El procedimiento también puede comprender la etapa de verificar si, para el parámetro de identificación única del dispositivo solicitante, el programa informático a instalar ya se ha transferido. Si no, el procedimiento puede proporcionar la transferencia del programa informático a dicho dispositivo. De lo contrario, se puede denegar la transferencia del programa informático a dicho dispositivo y/o se puede generar una señal.

Si el fabricante del microprocesador proporciona los parámetros de identificación única, se puede afirmar que el producto en particular en el mercado con resultado de verificación negativa no ha sido producido por una empresa autorizada y/o no ha sido autorizado de otra manera.

Breve descripción de los dibujos

La invención se entenderá mejor siguiendo la descripción y los dibujos adjuntos, que muestran realizaciones prácticas no limitantes de la invención. Más específicamente, en el dibujo:

Las Figuras 1 y 2, ya descritas, muestran dos diagramas de conexión de un dispositivo genérico a un servidor a través de Internet;

La Figura 3 muestra un diagrama de una parte de memoria de un dispositivo para el almacenamiento de un gestor de arranque;

La Figura 4 muestra un diagrama de bloques funcional de un programa informático cifrado o un generador de microprograma cifrado a partir de un código sin claves de cifrado y código de identificación;

Las Figuras 5 y 6 muestran dos diagramas de bloques funcionales de dos configuraciones diferentes de un sistema de comunicación entre un servidor interno asociado con un generador de programas informáticos cifrados y un dispositivo en el campo.

Divulgación detallada de las realizaciones

Algunas características de la arquitectura de cualquier microcontrolador forman la condición previa para la invención. Típicamente, un microcontrolador puede programarse con códigos adicionales (llamados "bits de fusible") en los que se establece un área de memoria que no puede leerse por instrumentos externos (programadores/depuradores) y no puede eliminarse. Esta es el área donde reside típicamente el gestor de arranque, es decir, el primer programa que se inicia al reiniciar el microcontrolador. Esto se hace para evitar que el gestor de arranque se dañe, elimine o corrompa, por ejemplo, como resultado de una intervención externa. Dado que reside en un área no accesible y no eliminable, se elimina la posibilidad de daños accidentales, involuntarios o fraudulentos del gestor de arranque.

Hay dos formas de acceder al código del gestor de arranque: escribir un código fraudulento, que permita realizar una copia de seguridad del gestor de arranque, o conectarse a un dispositivo de programación (por ejemplo, JTAG) e intentar hacer la copia de seguridad. En el primer caso, el gestor de arranque se negará a ejecutarlo porque no es válido, ya que no está cifrado con los parámetros esperados (que son desconocidos). En el segundo caso, el microcontrolador impedirá el acceso, ya que está protegido, y la única alternativa posible será eliminar todo el contenido del área del código del microcontrolador, eliminando de manera efectiva también la información que se desea recuperar, haciendo imposible la recuperación.

Una parte del área protegida está reservada para almacenar en texto plano una o más claves de cifrado del programa informático o microprograma requerido por el dispositivo, por ejemplo, un programa de aplicación. Solo el gestor de arranque puede acceder a esta parte del área protegida durante la ejecución del código o programa para leer la(s) clave(s) de cifrado que se usará(n) para descifrar cualquier código de aplicación (programa informático/microprograma), que debe ejecutar o cualquier otra cosa necesaria para un correcto funcionamiento del dispositivo o el programa.

Otra parte del área protegida se usa para almacenar uno o más parámetros de identificación única del dispositivo. La Figura 3 muestra esquemáticamente una memoria 21 de un microcontrolador genérico 20 que forma parte de un dispositivo electrónico. La memoria se divide en un área protegida 23 y un área no protegida 25. En la segunda, como se mencionó, residen uno o más programas de aplicación. Viceversa, en el área protegida 23 hay tres zonas dedicadas al almacenamiento del gestor de arranque (zona 26), la(s) clave(s) de cifrado (zona 27) y los parámetros de identificación única del dispositivo (zona 28).

En general, pueden usarse una o más claves de cifrado y uno o más parámetros de identificación única del dispositivo. A continuación, por simplicidad, siempre se hará referencia a una clave de cifrado y a un parámetro de identificación única del dispositivo, entendiéndose que ambos pueden ser múltiples, es decir, un dispositivo puede tener más de una clave de cifrado y/o más de un parámetro de identificación única también en combinación entre sí.

Por clave de cifrado se entiende cualquier clave, que puede usarse para cifrar y descifrar un programa informático o microprograma mediante un algoritmo de cifrado y/o descifrado. Por parámetro de identificación única se entiende cualquier parámetro, que permite la identificación única de un dispositivo dado. Un parámetro de identificación única puede consistir, por ejemplo, en una cadena de dígitos binarios. En general, cada dispositivo fabricado por la empresa propietaria de los conocimientos que se protegerán se marcará o identificará mediante un parámetro de identificación única diferente de todos los demás dispositivos.

Como quedará claro a partir de la siguiente descripción, la clave de cifrado y el parámetro de identificación única de un dispositivo genérico se controlan de acuerdo con la invención de una manera innovadora, para aumentar la protección de los conocimientos de la empresa propietaria de los conocimientos, aumentar la seguridad de la protección de datos sensibles, que incluye en particular los programas de aplicación y, en general, el programa informático/microprograma desarrollado por la empresa.

Las zonas de memoria 26, 27 y 28 del microcontrolador genérico 20 están definidas por el programador que escribe el gestor de arranque, que reservará en el nivel de enlace las tres zonas 26, 27 y 28, definiendo sus direcciones. El programador almacenará el gestor de arranque en la zona 26, mientras que las claves de cifrado y los parámetros de identificación única se pueden ingresar en las zonas 27 y 28 de cada microcontrolador en una etapa posterior. De esta manera, el programador no conoce el contenido de las zonas 27 y 28. Creará el gestor de arranque dejando las zonas 27 y 28 vacías o llenas de caracteres ficticios, que no tienen significado y se modificarán posteriormente. En otras realizaciones, el gestor de arranque, la clave de cifrado y el parámetro de identificación única se pueden insertar en una sola operación, en ciertas condiciones protegidas, como se describe a continuación. En otras realizaciones, el microcontrolador puede preprogramarse integralmente, con el gestor de arranque, la clave de cifrado y el parámetro de identificación única, por la empresa de fabricación del microcontrolador, diferente de la empresa que posee el conocimiento a proteger. En otras realizaciones, el fabricante del microcontrolador puede programar la clave de cifrado y el parámetro de identificación única, dejando libre el espacio de memoria para el gestor de arranque, que será programado por la empresa propietaria de los conocimientos a proteger o con el consentimiento y bajo el control de este último.

La actualización de uno o más programas informáticos o microprogramas residentes en el área no protegida 25 requiere el conocimiento de la clave de cifrado y el parámetro de identificación única del dispositivo. De esta manera, al proteger estos datos (claves de cifrado y parámetros de identificación única del dispositivo y su combinación), es imposible el uso fraudulento del gestor de arranque u otro programa informático o microprograma, por ejemplo, la actualización de programa informático o microprograma, ya que es imposible descifrarlos.

La invención se basa en la idea de proteger las claves de cifrado y los parámetros de identificación única de los dispositivos, de modo que no sean poseídos por personas ajenas a la empresa propietaria de los conocimientos y, por extensión, incluso desconocidos para estos últimos en el caso de generación y escritura automatizada de estos parámetros.

El uso de claves de cifrado y parámetros de identificación única de los dispositivos también permite, como se verá más adelante, el control de los dispositivos individuales, evitando una sobreproducción para la venta en mercados paralelos, la actualización de dispositivos no autorizados, la verificación de que el programa informático actualizado correcto está instalado en el dispositivo correcto o incluso la creación de versiones de programa informático ad hoc para dispositivos particulares.

Si el fabricante del microcontrolador programa el microcontrolador, como ocurre en algunas soluciones recientes, las áreas protegidas de la memoria del microcontrolador se llenan de códigos aleatorios, que pueden considerarse o tratarse como claves de cifrado. En otras arquitecturas, se proporcionan las llamadas áreas OTP (Programable por Única Vez) que se programan durante la producción del microcontrolador con códigos únicos que no están interrelacionados. Algunos chips contienen datos únicos para rastrear la producción: número de chip, posición en la oblea de silicio, semana de producción y otros; estos datos también pueden usarse para este propósito. En general, estas áreas se tratarán como las áreas protegidas 27 y 28 del diagrama de la Figura 3, es decir, contienen información que se recupera cuando se ejecuta el gestor de arranque, o para descifrar un nuevo programa informático o microprograma, y no se utilizan durante la programación del gestor de arranque o cualquier otro microprograma almacenado en la memoria del microcontrolador.

En general, el gestor de arranque no contiene las claves de cifrado. Si es robado, el algoritmo de cifrado puede rastrearse mediante ingeniería inversa. Sin embargo, esta información aún no es suficiente para descifrar cualquier programa informático o microprograma cifrado, ya que faltan la clave o las claves de cifrado. Como se mencionó, estas últimos no residen en el gestor de arranque; residen en el área protegida 27 o 28 de la memoria del microcontrolador de la cual, por las razones indicadas anteriormente, no se pueden recuperar.

Para evitar los riesgos relacionados con la apropiación de la clave de cifrado y los parámetros de identificación única, se genera automáticamente un gestor de arranque que contiene estos datos adicionales, a través de un programa dedicado a esta función. Este programa, definido a continuación como generador de programas, debe conocer lo siguiente:

- el número de parámetros generales que se deben ingresar (claves de cifrado y parámetros de identificación única del dispositivo para el que está destinado el gestor de arranque);
- la posición en el archivo (es decir, en el programa de gestión de arranque) de cada parámetro individual (claves de cifrado y parámetros de identificación única);
- dimensión mínima y máxima permitidas de cada parámetro;
- el criterio para llenar los espacios vacíos si los parámetros de identificación y las claves de cifrado no llenan completamente los espacios de memoria para estos parámetros;
- el procedimiento para crear un archivo válido y códigos de validación de los parámetros ingresados y del código completo con los respectivos parámetros y claves de cifrado, de modo que el microcontrolador pueda ejecutar el gestor de arranque generado por el generador de programas en la fase de arranque.

La Figura 4 muestra un diagrama funcional del generador de programas, representado por el bloque 31. Recibe en la entrada el parámetro de identificación única (ID, bloque 33) del dispositivo para el cual está destinado el gestor de arranque generado, la clave de cifrado (Claves, bloque 35) y el gestor de arranque (bloque 37) sin clave de cifrado y parámetro de identificación única. En la salida del generador de programas 31, se obtiene el gestor de arranque (bloque 39) que contiene la clave de cifrado (Claves) y el parámetro de identificación única (ID) del dispositivo para el que está destinado el gestor de arranque.

El gestor de arranque completo con clave de cifrado y parámetro de identificación única (bloque 39) se carga en el microcontrolador destinado al dispositivo correspondiente.

Esta operación puede evitarse si el microcontrolador está preprogramado, es decir, ya está provisto de claves de cifrado y parámetros de identificación almacenados en las zonas protegidas 27 y 28 (Figura 3) del microcontrolador.

Esta fase de programación del microcontrolador puede llevarse a cabo, por ejemplo, en una empresa externa que produce, en nombre de la empresa propietaria de los conocimientos técnicos a proteger, los dispositivos electrónicos en cuyo microcontrolador debe almacenarse el gestor de arranque. La empresa propietaria de los conocimientos, que suministra el gestor de arranque y el programa informático o microprograma de la aplicación, permite a la empresa de terceros, que puede ubicarse en un sitio de producción diferente y distante de la sede de la empresa propietaria de los conocimientos, programar los microcontroladores manteniendo el control del programa informático (gestor de arranque) y la protección de la propiedad intelectual respectiva, evitando también la sobreproducción de dispositivos destinados al mercado paralelo, con el procedimiento que se describe a continuación.

La protección de los datos sensibles, que consisten principalmente en la clave de cifrado o las claves de cifrado y los parámetros de identificación, se logra de la siguiente manera.

Para todos los dispositivos que se producirán o programarán, la empresa fabricante generará una solicitud de clave de cifrado. La empresa propietaria de los conocimientos a proteger crea una clave de cifrado "Clave" para cada dispositivo y un ID de parámetro de identificación única para cada solicitud, es decir, para cada dispositivo que se produzca o programe, y genera una base de datos que contiene al menos la información en relación con las claves de cifrado, combinadas con los respectivos ID de los parámetros de identificación única de los respectivos dispositivos. Los datos se almacenan de manera combinada: cada parámetro de identificación única de un dispositivo se combina con la clave de cifrado respectiva asociada con dicho dispositivo.

En algunas realizaciones, la base de datos que recopila esta información contiene, por ejemplo, un registro para cada dispositivo para el cual se autoriza o solicita la producción o programación por parte de la empresa de producción de terceros. Cada registro contiene la clave de cifrado relativa a ese dispositivo y el parámetro de identificación única de ese dispositivo. Por lo tanto, el registro proporciona una combinación de clave de cifrado y un parámetro de identificación única del dispositivo. Cada dispositivo tendrá en general una clave de cifrado diferente de los otros dispositivos, pero esto no es esencial. Lo importante es que cada dispositivo puede identificarse de manera única y distinguirse de los demás, mediante el parámetro de identificación única respectivo.

Esta base de datos debe residir en un área adecuadamente protegida del sistema de TI de la empresa propietaria de los conocimientos. El acceso a la base de datos se obtiene durante la creación de un código (gestor de arranque o un programa informático o microprograma diferente, por ejemplo, un programa de aplicación) que se instalará en un dispositivo determinado.

Si los microcontroladores de los dispositivos ya están programados por el fabricante del microcontrolador con las claves de cifrado y los parámetros de identificación correspondientes, el fabricante del microcontrolador deberá proporcionar a la empresa propietaria de los conocimientos a proteger la información que consiste en las claves y los

parámetros de identificación combinados entre sí, para que la empresa propietaria de los conocimientos pueda almacenar esta información en su base de datos protegida.

Dicho esto, existen dos procedimientos posibles para gestionar la información para programar un nuevo dispositivo en condiciones de seguridad:

- en el primer caso, el generador de programas que genera el programa informático (por ejemplo, el gestor de arranque) que se instalará en el dispositivo se encuentra en un área protegida, por ejemplo, en el sitio protegido de la empresa propietaria de los conocimientos a proteger. Esta situación se esquematiza en el diagrama de la Figura 5;
- en el segundo caso, el generador de programas que genera el programa informático que se instalará en el dispositivo se encuentra en el sitio de producción, es decir, en un área no protegida, por ejemplo, en los trabajos de una empresa de terceros que produce/programa los dispositivos en nombre de la empresa propietaria de los conocimientos. Esta situación se esquematiza en el diagrama de la Figura 6.

En el diagrama de la Figura 5, el número de referencia 41 indica un área protegida en la que residen los datos de la empresa propietaria de los conocimientos. El número de referencia 43 indica un área genérica no protegida, por ejemplo, el sitio donde se producen o programan los dispositivos. En el área protegida 41 se disponen los archivos con la base de datos que contiene los datos sensibles, que comprenden en particular las claves de cifrado y los parámetros de identificación única de los dispositivos. Este archivo está indicado por el número 45. El bloque indicado por 47 representa el archivo de programa informático/microprograma de la empresa, que incluye el(los) gestor(es) de arranque si es necesario.

Se puede acceder a los archivos 45, 47 por un servidor interno 49, adecuadamente protegido hacia el exterior, con técnicas de tipo conocido. El servidor interno 49 puede comprender un generador de programas, o puede interactuar con un generador de programas, representado esquemáticamente por el bloque 51 y denominado "Generador HEX" en la Figura 5. La separación en los bloques funcionales 51 y 49 es puramente una indicación, entendiéndose que el generador de programas "Generador HEX" puede ser parte de o residir en el servidor 49.

Como se mencionó, el generador de programas tiene la función de generar, por ejemplo, un gestor de arranque que comprende la clave de cifrado y el parámetro de identificación única del dispositivo en el que debe cargarse el gestor de arranque. En la práctica, el generador de programas 51 toma el programa informático, por ejemplo, un gestor de arranque sin clave de cifrado y el parámetro de identificación única, del archivo 47, además de la clave de cifrado y el parámetro de identificación única del dispositivo que se programará desde el archivo 45. En algunas realizaciones, el servidor 49 genera la clave de cifrado y el parámetro de identificación única durante la solicitud de programación de un microcontrolador de un dispositivo, por un lado, suministra estos datos al generador de programas 51 y, por otro, los almacena en la base de datos 45.

El generador de programas Generador HEX 51 genera un programa informático o microprograma, por ejemplo, un gestor de arranque, completo con clave de cifrado y parámetro de identificación. El programa así generado se envía, a través de cualquier canal adecuadamente protegido, indicado esquemáticamente por 53, hacia el área no protegida 43, por ejemplo, un sitio de producción.

La Figura 5 representa esquemáticamente en el sitio de producción 43 un dispositivo 57 a programar. El número 55 indica un programador (Herramienta de Programador). Esta última es una herramienta, conocida per se, que realiza físicamente la programación del dispositivo 57.

La transmisión del programa que contiene la clave de cifrado y el parámetro de identificación única puede ser en texto plano o cifrado. En el último caso, la clave de cifrado no puede ser la atribuida al dispositivo 57 en la fase de programación, ya que dicha clave aún no se conoce en el sitio de producción. Por lo tanto, el cifrado se realiza con una clave de cifrado elegida por el programador 55 y se puede comunicar a través del canal protegido 53 al servidor de la empresa 49, junto con los datos representativos de las credenciales del programador 55, por ejemplo, un código de identificación, que permite al servidor 49 determinar que la solicitud generada proviene de un programador autorizado. Si se programan varios sitios de producción y/o varios programadores 55, cada uno puede caracterizarse por su propio código de identificación y, por lo tanto, el servidor 49 puede conocer (y almacenar) para cada clave de cifrado y parámetro de identificación única relativo el programador desde el que se hizo solicitud. La clave de cifrado asociada con el programador 55 no puede ser enviada por el programador al servidor 49, sino almacenada en un área protegida en el sitio 41, por ejemplo en la base de datos 45, por ejemplo combinada con el código de identificación del programador respectivo.

En resumen, por lo tanto: la solicitud de un programa informático, por ejemplo un gestor de arranque, para que se programe un nuevo dispositivo 57, se envía al sitio protegido 41 a través del canal protegido 53. Cuando el servidor 49 ubicado en el sitio protegido 41 recibe una solicitud de este tipo, el servidor 49 realizará las siguientes operaciones:

- generar aleatoriamente al menos una clave de cifrado (Clave) para el dispositivo 57 a programar. La clave puede generarse mediante el uso de cualquier técnica conocida;
- generar al menos un parámetro de identificación única (ID) para el dispositivo 57 a programar;
- almacenar un nuevo registro que contiene la clave de cifrado combinada con el parámetro de identificación única en la base de datos 45;
- tomar el gestor de arranque del archivo 47. En general, el archivo 47 contendrá varios gestores de arranque, por ejemplo, para diferentes dispositivos y/o diferentes versiones del gestor de arranque. Preferentemente, se tomará el gestor de arranque más actualizado dedicado al tipo de dispositivo 57 a programar;
- se usará el generador de programas 51 para generar el archivo completo a enviar, que consiste en el gestor de arranque con la clave de cifrado y el parámetro de identificación única del dispositivo;
- se transmitirá en el canal seguro 53 el programa completo con la clave de cifrado y el parámetro de identificación única atribuido al dispositivo 57 a programar.

El programador 55 recibe el gestor de arranque desde el canal seguro 53 y lo carga en el microcontrolador del dispositivo 57. En este punto, el dispositivo está programado con un gestor de arranque que contiene una clave de cifrado dedicada al dispositivo único 57, identificado por el parámetro de identificación única respectivo. Si el gestor de arranque con la clave de cifrado y el parámetro de identificación única se han cifrado antes de la transmisión, el programador 55 puede descifrarlos, es decir, reescribirlos en texto plano antes de cargarlos en la memoria protegida del microcontrolador. Dado que el programador 55 no hace ninguna copia física de la información recibida, la apropiación ilegal de la información también se evita en el sitio de producción no protegido, donde la información está en tránsito desde el programador 55 al dispositivo 57.

En el caso representado esquemáticamente en la Figura 6, se hipotetiza que el generador del programa se coloca en el área no protegida, es decir, en el sitio de producción 43. En la Figura 6 números iguales indican partes iguales o equivalentes a las de la Figura 5. En esta configuración, un generador de programas 51A está presente en el área no protegida o sitio 43 y conectado, por medio de un canal protegido 58, al programador 55. En algunas realizaciones, los dos instrumentos (programador 55 y generador de programas 51A) pueden diseñarse como un único componente que tiene las dos funciones, de manera que el canal de comunicación protegido 58 entre los dos instrumentos ya no es necesario. El procedimiento de programación se describe a continuación con referencia a dos dispositivos separados 55 y 51A, pero el procedimiento será sustancialmente el mismo incluso si las funciones de estos dos dispositivos se incorporan en un solo instrumento.

En el diagrama de la Figura 6, se proporciona un generador de programas 51 también en el área protegida 41, para los fines que se aclararán más adelante.

Cuando se debe programar un nuevo dispositivo 57, el generador de programas 51A envía a través del canal protegido 53 una solicitud al servidor 49, proporcionando sus credenciales, por ejemplo, su número de identificación, conocido por el servidor 49. Si es necesario, también puede transmitir una clave de cifrado, o el servidor 49 puede conocer la clave de cifrado asociada con el generador de programas 51A.

El servidor 49 toma el gestor de arranque más apropiado del archivo 47 y lo envía a través del canal protegido 53. El gestor de arranque, en el que falta la clave de cifrado asociada con el dispositivo 57 a programar, es completada al menos en parte por el servidor 49 antes de la transmisión. En particular, el servidor 49 genera un parámetro de identificación única (ID) que se atribuye al dispositivo 57. Como en el caso descrito anteriormente, el gestor de arranque podría cifrarse antes de la transmisión en el canal protegido 53, por ejemplo, mediante una clave de cifrado asociada con el generador de programas 51A respectivo o con el programador 55 respectivo.

El generador de programas 51A recibe el gestor de arranque y lo compila insertando la clave de cifrado en él. Esta clave de cifrado debe ser conocida también por el servidor 49. De hecho, como en la configuración descrita con referencia a la Figura 5, también en este caso el servidor 49 debe almacenar en la base de datos 45 la combinación entre la clave de cifrado (Clave) y el parámetro de identificación única (ID) de cada dispositivo 57 programado. Los propósitos de esto se explicarán a continuación. Si bien el servidor 49 proporciona el parámetro de identificación única, la clave de cifrado se genera en el área no protegida 43 y, por lo tanto, debe darse a conocer de alguna manera al servidor 49, sin pasar por el canal 53.

Para dicho propósito, las técnicas conocidas per pueden usarse para la generación de claves idénticas en el servidor 49 y en el generador de programas 51A. Por ejemplo, el generador de programas 51A puede asociarse con un generador de números pseudoaleatorios. En cualquier momento es posible que el servidor 49 sepa qué número aleatorio es generado por el generador de números aleatorios de un generador de programas 51A dado. Si se proporcionan varios generadores de programas 51A, por ejemplo en diferentes sitios de producción, cada uno de ellos estará asociado con su propio generador de números pseudoaleatorios, siendo dichos generadores de números pseudoaleatorios diferentes entre sí, es decir, para generar secuencias de números pseudoaleatorios diferentes entre sí.

Cada generador de números pseudoaleatorios se caracteriza por una "semilla" (diferente para todos los generadores de números pseudoaleatorios) para la generación de los números pseudoaleatorios. En el diagrama de la Figura 6, el bloque 52 indica un generador de números pseudoaleatorio de este tipo. Cuando el generador de programas 51A tiene que programar un nuevo dispositivo 57, solicita al generador de números pseudoaleatorios 52 una o más claves de cifrado. La clave de cifrado estará dada por uno o por una secuencia de dichos números pseudoaleatorios. Además, el generador de programas 51A enviará al servidor 49 la solicitud para recibir un gestor de arranque, junto con sus credenciales. Para cada generador de programas 51A, el servidor conoce tanto la semilla para generar la secuencia de números pseudoaleatorios como el código de identificación que representa la credencial del generador de programas. Cuando el servidor 49 recibe una solicitud, por lo tanto, puede saber qué clave de cifrado ha generado el generador de números pseudoaleatorios 52 asociado con el generador de programas 51A que ha enviado la solicitud de transmisión de un gestor de arranque para programar un nuevo dispositivo 57) Por lo tanto, el servidor 49 puede almacenar en la base de datos 45 el registro que contiene el parámetro de identificación única del dispositivo 57 a programar (que ha sido asignado por el mismo servidor 49) y la clave de cifrado.

En resumen, por lo tanto, también en este caso el servidor 49 puede almacenar en la base de datos 45 la combinación del parámetro de identificación única (ID) del dispositivo 57 y la clave de cifrado relativa (Clave) para cada dispositivo fabricado y programado 57.

El programador 55 (Herramienta de Programador) provisto en las realizaciones de las Figuras 5 y 6 es en general una herramienta, que en la fase de producción se usa para programar físicamente el dispositivo 57 una vez que el gestor de arranque o en general el archivo de programa se ha obtenido del servidor 49.

Dado que el dispositivo 57 debe programarse con el programa en texto plano, es decir, no cifrado, el programador debe:

- proporcionar una conexión segura con el generador de programas que proporciona el gestor de arranque completo con clave de cifrado e identificación del dispositivo a programar;
- poseer una clave de identificación (soporte físico o similar) que permite a la empresa propietaria de los conocimientos identificar al programador de una manera única. Dicha clave puede usarse como clave de cifrado para el intercambio de información con el generador de programas (generador 51 en el caso de la Figura 5; generador 51A en el caso de la Figura 6);
- descifrar el archivo recibido para representarlo en texto plano y permitir la programación del dispositivo;
- no guardar en ningún formato y soporte el programa informático/microprograma recibido y transformado en texto sin formato;
- controlar el programador de acuerdo con las especificaciones del fabricante del programador y el microcontrolador a programar;
- evitar la programación de dos dispositivos con el mismo programa después de que la primera programación se ha realizado con éxito.

Estas características permiten a la empresa propietaria de los conocimientos mantener un rastro de los diferentes programadores 55, que pueden proporcionarse en diferentes áreas no protegidas 43 y de los dispositivos 57 que están realmente programados.

Si el generador de programas y el programador están configurados como una sola herramienta, las funciones descritas anteriormente se proporcionarán para dicha herramienta única.

Si es necesario aumentar la capacidad de producción por medio de un nuevo sitio de producción o un nuevo fabricante, todo lo que debe hacer la empresa propietaria de los conocimientos es proporcionar un nuevo programador 55 con su propia clave de identificación única, por ejemplo, una clave de soporte físico y almacene esta información en el archivo protegido, accesible por el servidor 49. Si la presencia del generador de programas 51A está programada en el sitio de producción, se proporcionará este componente, nuevamente con su propia clave de identificación o código de identificación.

El sistema descrito hasta ahora permite la programación segura de los dispositivos 57 con un gestor de arranque proporcionado por la empresa propietaria de los conocimientos, que tiene el control del servidor 49 y las bases de datos asociadas con él.

En algunos casos, el fabricante del chip puede programar el microcontrolador no solo con las claves de cifrado y, si es necesario, con el parámetro de identificación única, sino también con el gestor de arranque. En este caso, se omite la fase de programación del gestor de arranque descrita hasta ahora y la empresa propietaria de los conocimientos a proteger recibirá del fabricante de los microcontroladores que se instalarán en los dispositivos 57 toda la información que se almacenará en la base de datos 45, o los registros que contienen, para cada microcontrolador, la clave de cifrado y el parámetro de identificación única. El gestor de arranque también podría almacenarse en el archivo 47.

El gestor de arranque que se carga en los dispositivos individuales 57 generalmente puede ser de dos tipos:

- un gestor de arranque completamente cerrado: en este caso no se comunica de ninguna manera con el exterior;
- un gestor de arranque abierto con una ruta o canal de comunicación que permite la programación del primer programa.

La programación del programa informático/microprograma de la aplicación y las actualizaciones relacionadas en los dispositivos producidos 57 difieren de acuerdo con el tipo de gestor de arranque usado.

Si el gestor de arranque tiene un canal de comunicación con el exterior, una vez que el gestor de arranque se ha cargado en el dispositivo 57, puede recibir una aplicación de programa informático/microprograma y cargarlo en el dispositivo a través del canal de comunicación del gestor de arranque. Puede ser cualquier tipo de canal, por ejemplo, una conexión ethernet, serial, digital segura o inalámbrica, etc.

De acuerdo con el tipo de canal disponible, el gestor de arranque puede descargar el programa informático/microprograma de la aplicación directamente, a través de una conexión de ethernet, por ejemplo, y cargarlo en la memoria para que luego pueda ejecutarlo. El dispositivo 57 se conecta directamente y, a través del gestor de arranque, descarga el programa informático/microprograma de la aplicación. En el caso de un canal local (digital seguro) un operador descarga el programa informático o el microprograma de aplicación, lo coloca en una placa e inserta la placa en la carcasa del dispositivo 57 para que el gestor de arranque descargue el programa informático o el microprograma de aplicación desde la placa.

En ambos casos, el primer programa de aplicación (programa informático o microprograma) puede suministrarse por medio de un procedimiento similar al descrito con referencia a las Figura 5 y 6 para la programación del gestor de arranque (si no lo proporciona directamente el productor del microcontrolador). Cuando el dispositivo 57 se ha provisto de su propio gestor de arranque, que también contendrá el parámetro de identificación única (ID) asignado al dispositivo y la clave de cifrado (Clave) asignada al dispositivo, la transmisión del programa de aplicación (programa informático o microprograma) a cargar se puede solicitar, a través del canal 53. El procedimiento es el mismo que el descrito para enviar y cargar el gestor de arranque, la única diferencia es que en este punto, dado que tanto el parámetro de identificación única como la clave de identificación ya se han atribuido al dispositivo 57, estos datos no tienen que proporcionarse por el servidor 49. Además, la combinación de clave de cifrado (Clave) y parámetro de identificación única (ID) para el dispositivo en cuestión ya están almacenados en la base de datos 45.

El servidor 49 recibe la solicitud de un nuevo programa de aplicación que:

- recupera el programa de aplicación del archivo 47,
- si es necesario, recupera de la base de datos 45 la clave de cifrado asociada con el parámetro de identificación única del dispositivo 57 que envió la solicitud;
- si es necesario, cifra el programa de aplicación con dicha clave de cifrado;
- envía el programa de aplicación (cifrado, si es necesario) a través del canal 53 al programador 55.

El programa de aplicación cifrado se carga en el dispositivo 57. Si se ha enviado cifrado, aquí se descifrará por medio de la clave de cifrado que ya reside en el dispositivo, ya que se ha cargado en dicho dispositivo siguiendo uno de los procedimientos descritos anteriormente. La operación de descifrado debe realizarse dentro del dispositivo sin involucrar entidades externas (por ejemplo, memorias) que pueden proporcionar información sobre el procedimiento.

Si el gestor de arranque no tiene canal de comunicación, se deberá proporcionar un primer programa de aplicación durante la programación del gestor de arranque. En este caso, por lo tanto, el generador de programas 51 (Figura 5) o 51A (Figura 6) generará un archivo que es el resultado de la suma, la concatenación o, en general, cualquier combinación entre el gestor de arranque y el programa de aplicación inicial, es decir, de dos programas El archivo resultante puede cifrarse con la clave de cifrado asignada al programador 55 o al generador de programas 51A o no puede cifrarse. Este microprograma compuesto será programado por el programador 55 directamente en el dispositivo 57. El gestor de arranque y el programa de aplicación (después de descifrar si es necesario) se cargarán en la memoria del microcontrolador del dispositivo 57. Debido a que el gestor de arranque y el primer programa de aplicación pasan a través del programador 55 en texto plano, como se indicó anteriormente, el programador 55 no tendrá que hacer una copia del programa, evitando así generar agujeros en el sistema de seguridad. El programa en texto plano (gestor de arranque y programa de aplicación) nunca estará en una condición de manera que pueda extraerse y copiarse ilegalmente.

Al final de la operación, el dispositivo 57 se programará con el gestor de arranque, la clave de cifrado (Clave) y el parámetro de identificación única (ID), almacenados en el área protegida 23 (Figura 3) del microcontrolador y con un programa de aplicación en texto plano almacenado en el área no protegida 25.

Alternativamente, junto con el gestor de arranque puede proporcionarse un programa de aplicación "ficticio", es decir, un microprograma que no tiene otra función que no sea permitir que el dispositivo 57 descargue un programa de aplicación "real". En este caso, el dispositivo se inicia y el programa de aplicación "ficticio" lleva a cabo la solicitud al servidor 49 para que se reconozca un programa de aplicación actualizado mediante el uso del ID del dispositivo. Una vez que el dispositivo se ha reconocido, el servidor 49 lleva a cabo de forma segura el procedimiento ya

descrito, cifrando el microprograma con la clave de cifrado Clave asociada con el ID de parámetro de identificación única asociado con el dispositivo 57 durante la fase de programación y que ya se ha almacenado en el microcontrolador del dispositivo 57, así como también en la base de datos protegida 45 del sitio 41, donde se encuentra combinado con el parámetro de identificación única del dispositivo 57.

Si el microcontrolador se suministra ya programado con la clave de cifrado, el parámetro de identificación única y el gestor de arranque por el productor del microcontrolador, los procedimientos para programar el programa de aplicación son los mismos.

Cuando el dispositivo 57 se ha programado con su propio gestor de arranque, su propia clave de cifrado, su propio parámetro de identificación única y el programa de aplicación, puede instalarse en el campo y puede dialogar, a través de cualquier canal no protegido, con un servidor de monitoreo o con el propietario del dispositivo, por ejemplo también con el servidor 49. La conexión puede hacerse directamente o mediante un ordenador al que está conectado el dispositivo. A través de los datos atribuidos al dispositivo, y en particular el parámetro de identificación única, en el caso de la conexión a un servidor, es posible que la empresa que fabrica el dispositivo y que posee los conocimientos verifique, por ejemplo, si el dispositivo que está actualmente conectado en realidad corresponde a uno de los dispositivos que se han producido, o si es el resultado de una clonación o una sobreproducción no autorizada. También es posible verificar, por ejemplo, si se trata de un dispositivo en garantía, o para el cual se han firmado contratos de mantenimiento o actualización, etc. Todo esto permite que el cliente que usa físicamente el dispositivo se beneficie de una serie de servicios posventa.

En particular, es posible llevar a cabo actualizaciones del programa informático/microprograma con el que se proporciona el dispositivo, corregir defectos en el programa informático o microprograma inicial, proporcionar funciones adicionales solicitadas por el cliente o simplemente reemplazar un programa de aplicación obsoleto con otro más reciente

La actualización puede realizarse manualmente, con la intervención del personal operativo. Viceversa, la actualización puede realizarse en modo remoto por el cliente que compró el dispositivo y que descarga un programa informático o microprograma actualizado a través de Internet o correo electrónico o cualquier otro tipo de conexión. También es posible que la actualización se realice automáticamente, con el dispositivo 57 que está programado para solicitar directamente la actualización de su propio programa informático o microprograma.

En cada uno de estos casos, el microprograma o el programa informático tiene que salir del área protegida, representada esquemáticamente por el archivo 47 en la Figura 5 o 6, y se transfiere al dispositivo 57, a través de un canal de transmisión generalmente no protegido, o físicamente en un soporte de memoria suministrado al personal de soporte técnico en el campo. Esto puede constituir un agujero en el sistema de seguridad.

De acuerdo con la invención, el problema se resuelve como sigue. Sin embargo, la solicitud de actualización llega al servidor de la empresa propietaria de los conocimientos, por ejemplo, el servidor 49. En el caso de la actualización en línea, esto ocurre a través de una solicitud de Internet que puede llegar a un área no protegida y de acceso público, por ejemplo, un servidor público como el servidor 11 ilustrado en la Figura 2. Desde aquí, el servidor público 11 pasa la solicitud al servidor interno (servidor 3 en la Figura 2, servidor 49 en las Figuras 5 y 6). El parámetro de identificación única (ID) del dispositivo 57 que realizó la solicitud se combina con la solicitud de actualización, o dicho parámetro puede ser solicitado por el servidor 11 que recibe la solicitud para enviar una actualización y al que el dispositivo responde comunicándose con su parámetro de identificación única Cuando la actualización se realiza manualmente, el operador le pedirá al servidor (por ejemplo, siempre el servidor público 11) que proporcione el programa informático/microprograma actualizado, indicando también el parámetro de identificación única de cada dispositivo a actualizar.

La solicitud, enviada al servidor interno 49 ubicado en el área protegida 41, es gestionada por el servidor interno 49 de la siguiente manera.

En primer lugar, la clave de cifrado (Clave) combinada con el parámetro de identificación única (ID) del dispositivo 57 para el que se destina la actualización se recupera de la base de datos 45, mientras que el programa informático/microprograma actualizado que se suministrará al dispositivo 57 puede recuperarse del archivo 47. El generador de programas 51 genera el programa cifrado, mediante el uso de la clave de cifrado recuperada y asociado solo con el dispositivo 57 que ha solicitado la actualización.

En este punto, el programa cifrado puede transmitirse o transferirse al dispositivo 57 de cualquier manera, también por medio de un canal no protegido o por medio del personal a cargo del soporte técnico, mantenimiento o actualización. El archivo transferido no puede descifrarse, ya que no contiene la clave de cifrado. Solo el dispositivo 57 puede descifrar el programa informático/microprograma, ya que la clave de cifrado está almacenada allí, la misma clave que el servidor 49 ha recuperado de la base de datos 45 y a través de la cual el generador de programas 51 ha cifrado el programa informático/microprograma actualizado. Para esto, se usa la base de datos 45 en la que la clave de cifrado respectiva está asociada con cada parámetro de identificación única de un dispositivo 57.

Si el programa informático o microprograma se suministra a un dispositivo diferente del identificado por el parámetro de identificación única (ID), dicho dispositivo no podrá descifrarlo, ya que no posee la clave de cifrado con la que se ha cifrado el programa informático o microprograma . El programa informático o microprograma cifrado destinado a un dispositivo específico no puede ser descifrado por ningún otro dispositivo que no posea la clave de cifrado correcta.

De esta manera, la seguridad del canal de transmisión o del operador en general, que también puede ser un operador asignado a la actualización de los dispositivos en el campo, se vuelve irrelevante. Cuando el operador es un operador, no posee la clave de cifrado y, por lo tanto, no puede llevar a cabo la ingeniería inversa del programa informático o microprograma que posee y no puede instalarlo en ningún dispositivo aparte del único dispositivo autorizado para recibir el programa informático actualizado o microprograma, que es el único dispositivo que posee la clave de cifrado.

El procedimiento descrito también puede usarse durante la producción de los dispositivos, o durante el reacondicionamiento o mantenimiento.

Como parece claro en la descripción hasta ahora, el procedimiento descrito aumenta la seguridad de la protección de la información de la empresa propietaria de los conocimientos en varios aspectos, previniendo o, en cualquier caso, limitando el riesgo de usos fraudulentos del conocimiento, como se resume a continuación.

Si la producción se delega en uno o más sitios de producción de subcontratación, a menudo sucede que este último intenta producir una mayor cantidad de dispositivos que los que realmente ordenó la empresa propietaria de los conocimientos, por ejemplo, para vender estos dispositivos adicionales en un mercado paralelo. Normalmente, el sitio de producción tiene toda la información y los materiales necesarios, que incluyen la lista de materiales, los productos semiacabados, los planes de montaje y el programa informático o microprograma que a menudo constituyen la parte más importante y valiosa de la tecnología a proteger. Si el sitio de producción de subcontratación tiene buenos contactos con los proveedores de los materiales y productos semiacabados, es relativamente fácil adquirir este último en exceso con respecto a la producción acordada con la empresa propietaria de los conocimientos a proteger. El sitio de producción de subcontratación normalmente también posee el programa informático en texto plano que se puede instalar en cualquier cantidad de dispositivos, creando así una sobreproducción para mercados paralelos sustancialmente sin límites.

Al adoptar un sistema de acuerdo con la invención, esto se evita. De hecho, el sitio de producción puede descargar a través del canal de conexión con la empresa propietaria de los conocimientos solo un programa informático o microprograma cifrado destinado a un dispositivo dado, caracterizado por una clave de cifrado dada que pertenece solo a ese dispositivo.

Se supone que un experto en programa informático, incluso en ausencia de programa informático en texto plano, puede clonar el microcontrolador programado, es decir, puede instalar el mismo programa informático o microprograma con la misma clave de cifrado en un dispositivo diferente al específico para el que se destina el programa informático, identificado por el parámetro de identificación única. Por lo tanto, se producirán dos dispositivos idénticos, con el mismo programa informático y la misma clave de cifrado, y también con el mismo parámetro de identificación única.

En la base de datos protegida 45, accesible solo por el servidor interno 49, se almacena un registro que contiene el parámetro de identificación única y la clave de cifrado única. El servidor 49 también puede almacenar en la base de datos protegida 45, o en otro archivo protegido, información sobre las actualizaciones descargadas por cada dispositivo, teniendo así disponible en todo momento una situación actualizada del estado de cada dispositivo en el campo, incluyendo información sobre qué versión de programa informático o microprograma está instalada en cada dispositivo identificado por su propio parámetro de identificación única. El programa informático de gestión del sistema está diseñado para evitar que el mismo dispositivo, es decir, un dispositivo con el mismo parámetro de identificación única, se actualice dos veces con el mismo programa informático/microprograma.

Si existen dos dispositivos idénticos en el campo, uno original y el otro clonado, cuando uno de los dos ha realizado la actualización, descargando el programa informático/microprograma del sitio web de la empresa propietaria de los conocimientos, el segundo dispositivo ya no puede actualizarse. De hecho, cuando el servidor 49 recibe la segunda solicitud de actualización, la base de datos del servidor 49 contendrá la información de que el dispositivo solicitante ya se ha actualizado y, por lo tanto, se evitará una segunda actualización. Al mismo tiempo, será posible identificar el dispositivo, si es necesario, saber dónde está instalado y de qué sitio de producción de subcontratación proviene, identificando así la fuente de los dispositivos producidos ilegalmente.

Supongamos que, por alguna razón, los microcontroladores se producen con una codificación única regular (clave de cifrado y parámetro de identificación única ID) y que estos microcontroladores están en manos de un sitio de producción de subcontratación que desea crear una sobreproducción. En este caso, se pueden producir dispositivos únicos (cada uno con su propio parámetro de identificación única y clave de cifrado). Sin embargo, en este caso, los datos (ID y clave) de estos dispositivos excedentes no están presentes en la base de datos 45 de la empresa

propietaria de los conocimientos. Por lo tanto, no pueden recibir ningún programa de aplicación ni actualizarse, ya que la solicitud de un programa informático/microprograma (ya sea un primer programa de aplicación o una actualización) no se borrará, ya que el servidor 49 no reconoce el parámetro de identificación única como válido. El dispositivo ilegal puede ser identificado y localizado.

Las situaciones descritas anteriormente permiten la identificación de un dispositivo producido ilegalmente cuando se conecta al servidor 49 de la empresa propietaria de los conocimientos, o cuando esta conexión se establece por un ordenador a través de la cual se descargará el programa informático/microprograma que se instalará.

Supongamos ahora que quien posee el dispositivo producido ilegalmente es lo suficientemente cauteloso y nunca se conecta al servidor 49 de la empresa propietaria de los conocimientos. Si el dispositivo necesariamente tiene que actualizarse, el programa informático/microprograma debe obtenerse sin pasar por el servidor 49. En una situación tradicional esto es posible. En el caso de un sistema de acuerdo con la invención, viceversa, la actualización es prácticamente imposible. De hecho, incluso si el titular del dispositivo producido ilegalmente pudiera obtener una versión actualizada del programa informático/microprograma, esto se cifraría con una clave de cifrado diferente de la almacenada en el dispositivo producido ilegalmente.

El sistema descrito y los procedimientos permiten obtener las siguientes mejoras:

- el microprograma o programa informático, que contiene la parte más importante de los conocimientos de la empresa, está protegido contra la ingeniería inversa;
- el programador de programa informático o microprograma ya no es uno de los puntos críticos de las claves de seguridad;
- el sitio de producción de subcontratación puede gestionarse de forma segura;
- la empresa propietaria de los conocimientos puede saber exactamente cuántos dispositivos se han producido y están presentes en el mercado;
- la empresa propietaria de los conocimientos puede garantizar el correcto mantenimiento de los dispositivos en el campo;
- la empresa propietaria de los conocimientos puede verificar si existe un dispositivo producido ilegalmente en el campo y localizarlo;
- pueden gestionarse las políticas para la actualización del microprograma y los contratos de mantenimiento y garantía.

Se entiende que el dibujo solo muestra un ejemplo proporcionado únicamente como una demostración práctica de la invención, que puede variar en sus formas y disposiciones sin apartarse del ámbito del concepto subyacente a la invención. La presencia de números de referencia en las reivindicaciones adjuntas tiene el propósito de facilitar la lectura de la reivindicación con referencia a la descripción y al dibujo, y no limita el ámbito de la protección representada por las reivindicaciones.

REIVINDICACIONES

1. Un sistema para gestionar dispositivos electrónicos programables, que comprende:
- una pluralidad de dispositivos electrónicos (57), cada uno identificado por al menos un parámetro de identificación única (ID) y que contiene al menos una clave de cifrado (Clave);
- al menos un sitio protegido (41), en el que:
o reside una base de datos protegida (45), en la que para cada uno de dichos dispositivos electrónicos (57) el parámetro de identificación única (ID) y la clave de cifrado (Clave) se almacenan de manera combinada, de modo que cada parámetro de identificación única de un dispositivo electrónico se combina con la respectiva clave de cifrado asociada con dicho dispositivo electrónico;
o y se proporciona un archivo de programa informático/microprograma (47);
- un servidor (49) programado para:
o recibir de uno de dichos dispositivos electrónicos (57) una solicitud de transmisión de un programa informático almacenado en dicho archivo de programa informático/microprograma;
o recuperar de la base de datos protegida (45) la clave de cifrado asociada con el parámetro de identificación única del dispositivo electrónico (57) desde el cual se recibió la solicitud;
o recuperar el programa informático solicitado del archivo;
o generar una versión cifrada de dicho programa informático, mediante el uso de la clave de cifrado (Clave), que en dicha base de datos (45) se combina con el parámetro de identificación única (ID) del dispositivo electrónico (57) que ha solicitado la transmisión de dicho programa informático;
o enviar el programa informático cifrado al dispositivo electrónico; dicho dispositivo electrónico que se adapta para descifrar el programa informático cifrado mediante el uso de dicha clave de cifrado e instalar el programa informático.

2. Sistema como se reivindicó en la reivindicación 1, en el que dicho servidor (49) está programado para almacenar información relativa a la transmisión del programa informático a dichos dispositivos, y para subordinar la transmisión de un programa informático solicitado por uno de dichos dispositivos (57) a al menos una condición definida por dicha información.

3. Sistema como se reivindicó en la reivindicación 1 o 2, en el que dicho servidor (49) está programado para evitar una segunda transmisión de un programa informático a un dispositivo (57) al que dicho programa informático ya se ha enviado una vez.

4. Sistema como se reivindicó en una o más de las reivindicaciones anteriores, que comprende al menos un sitio de producción (43), diferente de dicho sitio protegido (41), un programador (45) que se proporciona en dicho sitio de producción (43), diseñado para recibir un programa informático desde dicho servidor (49) y programar dichos dispositivos (57) con dicho programa informático.

5. Sistema como se reivindicó en la reivindicación 4, en el que se proporciona un generador de programas (51A) en dicho sitio de producción (43).

6. Sistema como se reivindicó en una o más de las reivindicaciones anteriores, en el que se proporciona un generador de programas (51) en dicho sitio protegido para generar un programa informático asociado con un parámetro de identificación única (ID) de uno de dichos dispositivos (57) y con una clave de cifrado (Clave) correspondiente a dicho parámetro de identificación única (ID).

7. Sistema como se reivindicó en una o más de las reivindicaciones anteriores, en el que dicho servidor (49) está programado para: recibir una solicitud de un programa informático por parte de uno de dichos dispositivos (57), comprendiendo dicha solicitud al menos el parámetro de identificación única (ID) del dispositivo solicitante; verificar si el parámetro de identificación única (ID) del dispositivo (57) que solicitó dicho programa informático está contenido en dicha base de datos protegida (45); si el parámetro de identificación única (ID) del dispositivo solicitante (57) está contenido en la base de datos protegida (45), verificar al menos una condición de habilitación de actualización del dispositivo solicitante (57); si se cumple dicha condición, enviar a dicho dispositivo solicitante (57) una versión del programa informático solicitado cifrada con la clave de cifrado (Clave) asociada con el parámetro de identificación única (ID) del dispositivo solicitante (ID).

8. Sistema como se reivindicó en una o más de las reivindicaciones anteriores, en el que dicho servidor (49) está programado para suministrar un gestor de arranque a cada uno de dichos dispositivos (57).

9. Sistema como se reivindicó en la reivindicación 8, en el que dicho servidor (49) está programado para suministrar a cada uno de dichos dispositivos (57) un gestor de arranque asociado con una clave de cifrado (Clave).

10. Sistema como se reivindicó en la reivindicación 8 o 9, en el que dicho servidor (49) está programado para suministrar a cada uno de dichos dispositivos (57) un gestor de arranque asociado con un parámetro de identificación única (ID) de dichos dispositivos.

11. Sistema como se reivindicó en la reivindicación 8 o 9 o 10, en el que dicho servidor (49) está programado para suministrar a cada uno de dichos dispositivos (57) dicho gestor de arranque en versión cifrada.

12. Un procedimiento para instalar un programa informático en una pluralidad de dispositivos electrónicos (57), que comprende las etapas de:
- almacenar en cada dispositivo electrónico (57) al menos un parámetro de identificación única (ID) y al menos una clave de cifrado (Clave);
- en una base de datos protegida (45) proporcionada en un sitio protegido (41), almacenar para cada dispositivo (57) el respectivo parámetro de identificación única (ID) y la respectiva clave de cifrado (Clave) de manera combinada, de modo que cada parámetro de identificación única de cada uno de dichos dispositivos electrónicos se combina con la clave de cifrado respectiva asociada con el dispositivo electrónico respectivo;
- proporcionar un archivo de programa informático/microprograma (47) en dicho sitio protegido (41);
- proporcionar un servidor (49) en dicho sitio protegido (41);
- recibir en dicho servidor (49) una solicitud de un programa informático de uno de dichos dispositivos electrónicos (57);
- recuperar de la base de datos protegida (45) la clave de cifrado asociada con el parámetro de identificación única del dispositivo (57) desde el cual se recibió la solicitud;
- recuperar el programa informático solicitado del archivo;
- cifrar el programa informático recuperado que se va a instalar en el dispositivo electrónico (57) que solicita el programa informático, con la clave de cifrado (Clave) correspondiente al parámetro de identificación única (ID) de dicho dispositivo electrónico (57) que solicita dicho programa informático, obtener un programa informático cifrado;
- transferir dicho programa informático cifrado a dicho dispositivo electrónico (57) que solicita el programa informático;
- descifrar dicho programa informático en dicho dispositivo electrónico (57) que solicita el programa informático mediante el uso de dicha clave de cifrado (Clave) e instalar el programa informático en dicho dispositivo electrónico (57).

13. El procedimiento como se reivindicó en la reivindicación 12 que comprende además, las etapas de:
- generar una solicitud de un programa informático por uno de dichos dispositivos (57), dicha solicitud que comprende al menos el parámetro de identificación única (ID) del dispositivo solicitante (57);
- verificar si el parámetro de identificación única (ID) del dispositivo (57) que ha solicitado dicho programa informático está contenido en dicha base de datos protegida (45);
- si el parámetro de identificación única (ID) del dispositivo solicitante (57) está contenido en la base de datos protegida (45), verificar si dicho dispositivo solicitante (57) cumple al menos una condición de habilitación de actualización;
- si se cumple la condición, enviar a dicho dispositivo solicitante (57) una versión del programa informático solicitado cifrada con la clave de cifrado (Clave) combinada con el parámetro de identificación única (ID) del dispositivo solicitante (ID) y recuperado de dicha base de datos protegida (45);
- si no se cumple la condición, no enviar el programa informático solicitado al dispositivo solicitante.

14. El procedimiento como se reivindicó en la reivindicación 12 o 13, que comprende las etapas de:
- verificar si para el parámetro de identificación única (ID) del dispositivo solicitante, el programa informático a instalar ya se ha transferido;
- si no, transferir el programa informático a dicho dispositivo (57);
- en caso afirmativo, denegar la transferencia del programa informático a dicho dispositivo y/o generar una señal.

Figura 1

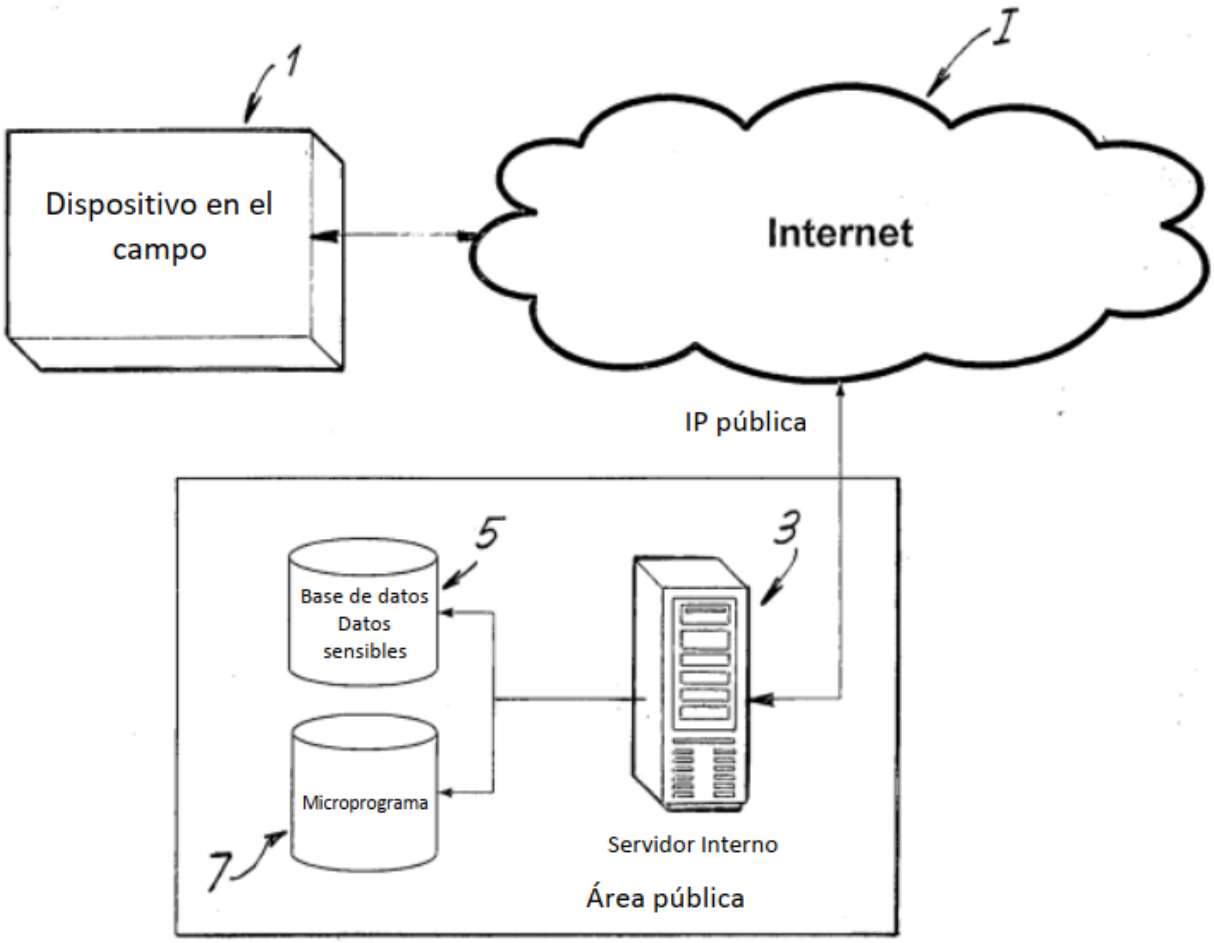
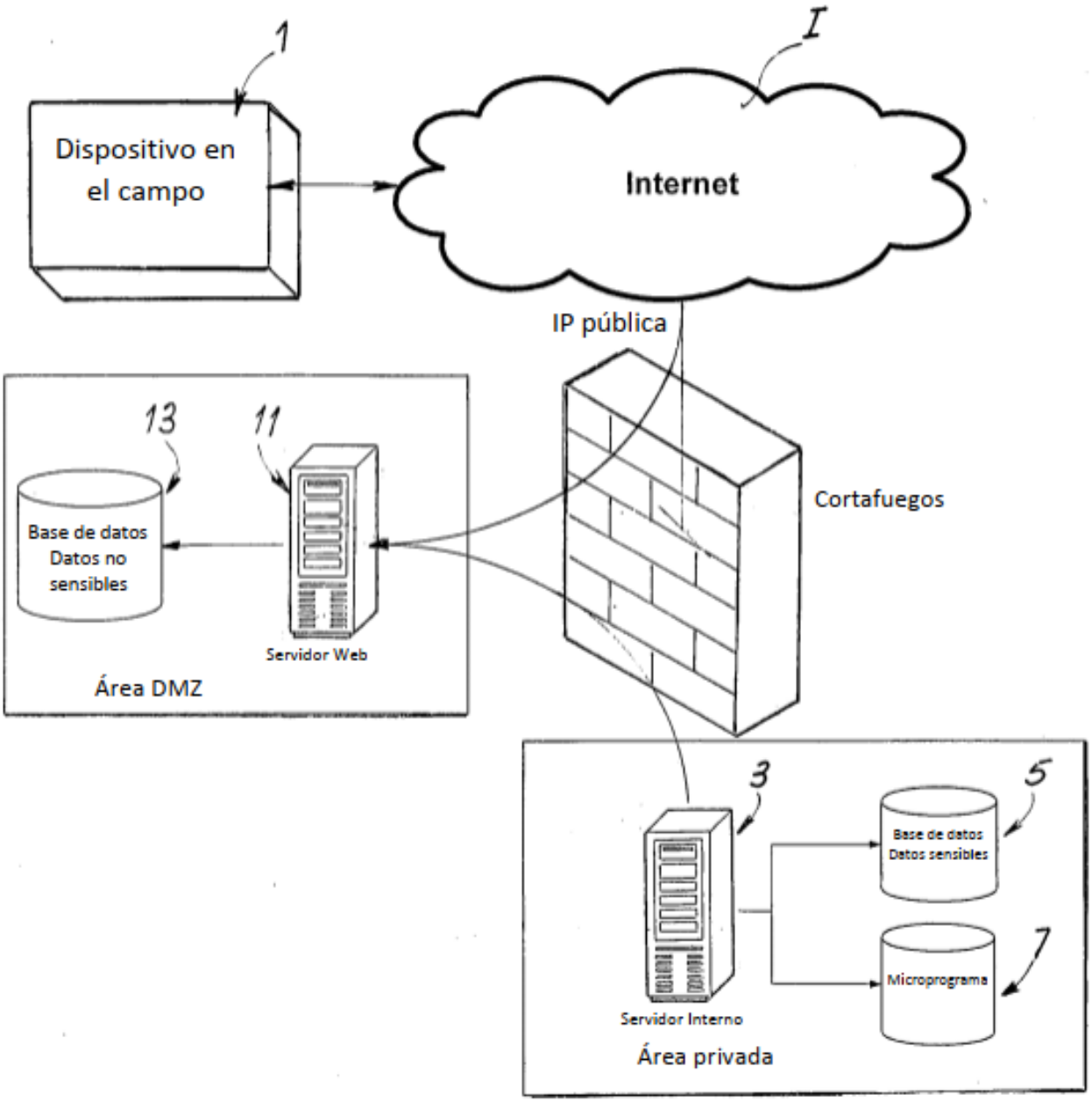

1
I
Dispositivo en el campo
Internet
IP pública
5
3
Base de datos
Datos
sensibles
Microprograma
7
Servidor Interno
Área pública

Figura 2


1
I
Dispositivo en el campo
Internet
IP pública
13
11
Base de datos Datos no sensibles
Servidor Web
Área DMZ
Cortafuegos
3
5
Base de datos Datos sensibles
Microprograma
7
Servidor Interno
Área privada

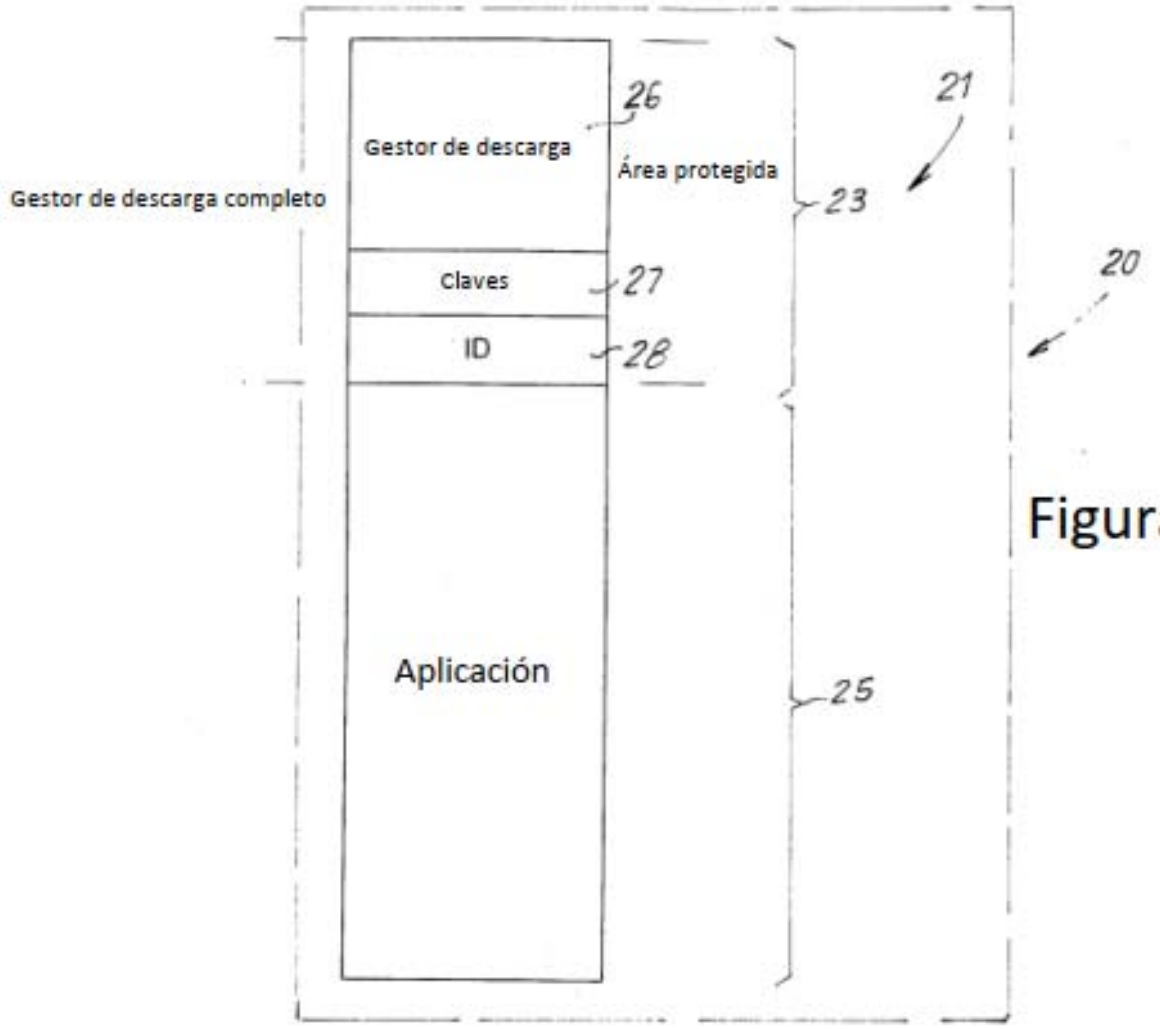


Figura 3

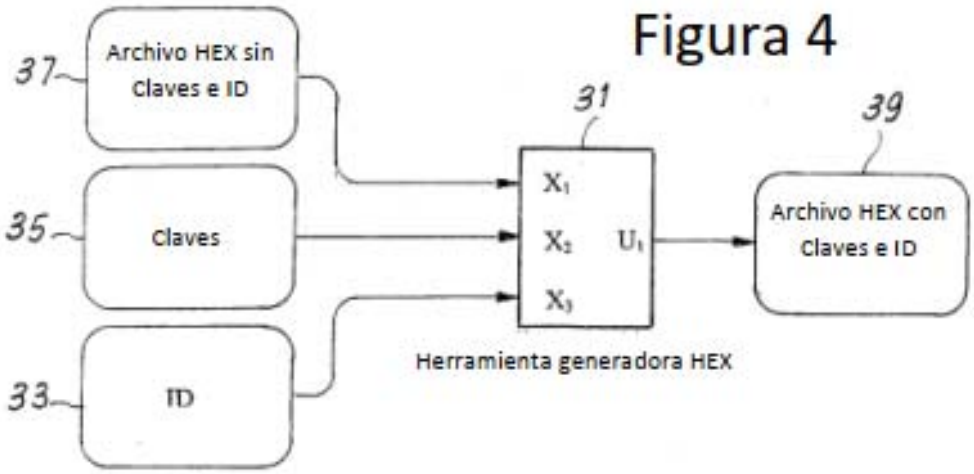


Figura 4

Figura 5

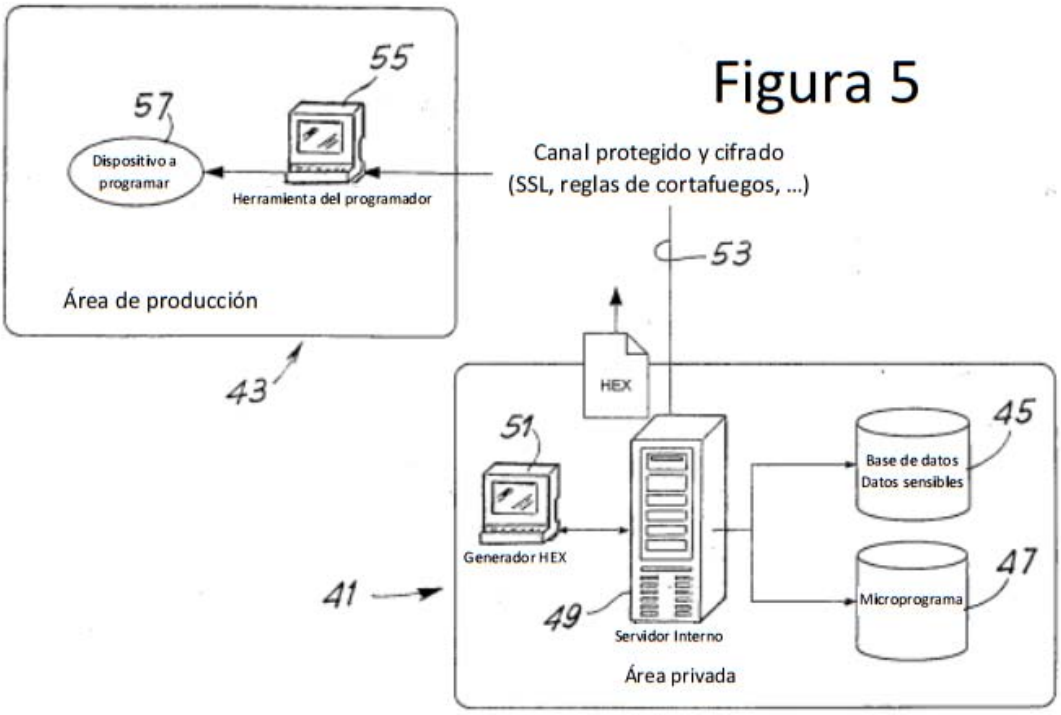


Figura 6