(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 733 075**

(51) Int. CI.:

G06F 21/85 (2013.01)
G06F 21/44 (2013.01)
G06F 21/62 (2013.01)
G06F 21/34 (2013.01)
G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **16.09.2015 E 15382450 (3)**

(97) Fecha y número de publicación de la concesión europea: **27.03.2019 EP 3144841**

(54) Título: **Sistema, método y dispositivo para evitar ataques cibernéticos**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.11.2019

(73) Titular/es:

FUNDACIÓN TECNALIA RESEARCH & INNOVATION (100.0%)
Parque Científico y Tecnológico de Gipuzkoa, Mikeletegi Pasealekua, 2
20009 San Sebastián, Gipuzkoa, ES

(72) Inventor/es:

GAMINO GARCÍA, ARKAITZ;
EGUÍA ELEJABARRIETA, IÑAKI;
LÓPEZ CARRERA, ÁNGEL;
REGO FERNÁNDEZ, ÁNGEL y
DEL RÍO DEL RÍO, IDOYA

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

Observaciones:

Véase nota informativa (Remarks, Remarques o Bemerkungen) en el folleto original publicado por la Oficina Europea de Patentes

DESCRIPCIÓN

Sistema, método y dispositivo para evitar ataques cibernéticos

Campo técnico

La presente invención se refiere al campo de la seguridad en redes informáticas, en particular en redes informáticas industriales. Más precisamente se refiere a métodos y sistemas para evitar ataques originados en sistemas de almacenamiento de datos, tales como dispositivos de USB.

Estado de la técnica

Las plantas y operadores industriales han sufrido de muchos tipos de ataques en el pasado. Estos ataques se llevaron a cabo consiguiendo acceso físico a servicios críticos, realizando a continuación sabotaje, espionaje o ataques terroristas. Las medidas de seguridad tradicionales se han centrado en soluciones perimetrales físicas, determinando con precisión los sistemas de control de acceso y sistemas de detección de intrusión como herramientas de salvaguarda primarias.

Los ataques han evolucionado después de la adopción por las infraestructuras industriales y críticas de los protocolos de TCP/IP y las tecnologías de información y comunicación novedosas. Al abarcar la ICT (tecnología de la información y las comunicaciones) implica mejorar la productividad y la eficacia, pero también conlleva obtener vulnerabilidades intrínsecas a la tecnología que podrían aprovecharse. De hecho, ataques bien conocidos, tales como Stuxnet, aprovechan tanto barreras físicas como lógicas. En particular, Stuxnet, el ataque más devastador en la última década, combinaba penetración de barreras físicas y lógicas. Stuxnet y ataques similares realizados en los últimos años tienen un origen de ataque común: acceso de USB en los recursos de la industria operacionales.

Los recursos de la industria no funcionan al mismo nivel de seguridad que lo hacen los recursos corporativos, el requisito principal de los sistemas de operación industrial es la disponibilidad en lugar de la seguridad. Los sistemas de operación industrial se ejecutan frecuentemente junto con software sin parchear y/o en sistemas operativos desactualizados y arcaicos. Esto significa que muchos dispositivos y conexiones (tales como servidores, PLC, RTU, MTU, BES, IED, protocolos industriales, etc.) no resuelven las vulnerabilidades de seguridad como deberían. La industria está intentando resolver esto de dos maneras: (1) aislando redes internas (redes operacionales) del resto del mundo (incluso de redes corporativas); en este sentido, se usan nuevas soluciones de pasarela de diodo y cortafuegos industriales para tal aislamiento; y (2) monitorización a través de soluciones SIEM (Información de Seguridad y Gestión de Eventos), para intentar reaccionar tan pronto como sea posible cuando tiene lugar un brote.

Ni estas soluciones ni las soluciones de antivirus tradicionales (puesto que no pueden desplegarse en el campo operacional) pueden evitar los ataques mencionados.

El documento W02015/000967A1 desvela un dispositivo, sistema y método para asegurar la transferencia de datos entre un dispositivo de almacenamiento de datos portátil seguro y un sistema informático de destino, que requiere un medio de almacenamiento de datos externo intermedio para transferir los datos del dispositivo de almacenamiento de datos portátil seguro a este medio de almacenamiento de datos externo intermedio.

La publicación por Bo Yang et al “TMSUI: A Trust Management Scheme of USB Storage Devices for Industrial Control Systems”, International Association for Cryptologic Research, 2015, desvela un sistema para proteger Sistemas de Control Industrial contra software malicioso en dispositivos de almacenamiento de USB. El sistema usa características de autenticación y autorización, que incluyen listas blancas para dispositivos de almacenamiento de USB autorizados.

Por lo tanto, existe una necesidad de un sistema, método y dispositivo para evitar ataques originados en sistemas de almacenamiento de datos, principalmente en redes industriales.

Descripción de la invención

Es un objetivo de la invención proporcionar un sistema, método y dispositivo para evitar ataques cibernéticos. En particular, el sistema y método controlan y trazan el manejo de los sistemas de almacenamiento de datos, tal como dispositivos de USB, asociados a trabajadores, operadores y visitantes principalmente en la industria, y evita ataques originados en estos sistemas de almacenamiento de datos. El método y sistema de la invención permiten controlar el uso de dispositivos de almacenamiento de datos en cualquier sistema, pero en particular en sistemas de operación industriales, en los que un ataque que conduce a la denegación de servicios esenciales (tales como electricidad, gas, agua...) podría producir un impacto principal.

De acuerdo con un aspecto de la presente invención, se proporciona un sistema de seguridad para evitar ataques cibernéticos en un sistema que comprende una pluralidad de dispositivos informáticos. El sistema de seguridad comprende: al menos un dispositivo de control que comprende: medios para autenticar a un usuario que intenta

acceder físicamente a una zona que comprende al menos un dispositivo informático de la pluralidad de dispositivos informáticos; medios para autenticar a un dispositivo de almacenamiento de datos que el usuario pretende insertar en al menos uno de estos dispositivos informáticos y para verificar, limpiar y encriptar el contenido del dispositivo de almacenamiento de datos; medios para, si el dispositivo de almacenamiento de datos llevado por el usuario es un dispositivo de almacenamiento de datos privado, proporcionar un dispositivo de almacenamiento de datos corporativo, en el que el dispositivo de almacenamiento de datos corporativo proporcionado comprende una copia del contenido originalmente almacenado verificado, limpiado y encriptado en el dispositivo de almacenamiento de datos privado. El sistema de seguridad también comprende un agente de software instalado en al menos uno de la pluralidad de dispositivos informáticos. El agente de software está configurado: para detectar si un dispositivo de almacenamiento de datos insertado en un puerto del dispositivo informático es uno privado o uno corporativo; para, en el caso de uno privado, denegar el acceso del dispositivo de almacenamiento de datos a ese dispositivo informático; y para, en el caso de uno corporativo, comprobar si su contenido se ha verificado, limpiado y encriptado por un dispositivo de control y, en el caso en que lo haya sido, desencriptar el contenido del dispositivo de almacenamiento de datos corporativo, permitiendo por lo tanto que el dispositivo informático lea o ejecute ese contenido.

El dispositivo de almacenamiento de datos puede ser una unidad de USB, o una mini unidad de USB, o una micro unidad de USB, o un DVD, o un CD, o una tarjeta SD, o una mini tarjeta SD o una micro tarjeta SD, o un disco duro portátil, o cualquier otro formato del sistema de almacenamiento de datos.

En una realización particular, los medios para autenticar a un usuario comprenden medios para leer una tarjeta de acceso o un identificador electrónico del usuario, en el que los medios para leer una tarjeta o un identificador electrónico comprenden una ranura para insertar una tarjeta o un lector inalámbrico para detectar inalámbricamente la información registrada en la tarjeta o en el identificador electrónico.

En una realización preferida, el sistema de seguridad comprende adicionalmente al menos un adaptador que comprende un primer puerto configurado para recibir un dispositivo de almacenamiento de datos externo y un segundo puerto configurado para enchufarse en un correspondiente puerto de un dispositivo informático de la pluralidad de dispositivos informáticos. El adaptador proporciona una interfaz física entre el dispositivo de almacenamiento de datos externo y el dispositivo informático mientras que aísla el dispositivo informático del dispositivo de almacenamiento de datos externo. Más preferentemente, el adaptador comprende medios para detectar si el dispositivo de almacenamiento de datos insertado en el puerto del adaptador es uno privado o uno corporativo; para, en el caso de uno privado, denegar el acceso del dispositivo de almacenamiento de datos a ese dispositivo informático; y para, en el caso de uno corporativo, comprobar si su contenido se ha verificado, limpiado y encriptado por un dispositivo de control y, en el caso en que lo haya sido, desencriptar el contenido del dispositivo de almacenamiento de datos, permitiendo por lo tanto que el dispositivo informático lea o ejecute ese contenido.

En otro aspecto de la invención, se proporciona un método para evitar ataques cibernéticos en un sistema que comprende una pluralidad de dispositivos informáticos. El método comprende: en al menos un dispositivo de control: autenticar un usuario que intenta acceder físicamente a una zona que comprende al menos parte del sistema que comprende una pluralidad de dispositivos informáticos; autenticar un dispositivo de almacenamiento de datos que el usuario pretende insertar en al menos uno de estos dispositivos informáticos y verificar, limpiar y encriptar el contenido del dispositivo de almacenamiento de datos, en el que el dispositivo de almacenamiento de datos es uno corporativo o uno privado; si el dispositivo de almacenamiento de datos llevado por el usuario es un dispositivo de almacenamiento de datos privado, proporcionar un dispositivo de almacenamiento de datos corporativo, en el que el dispositivo de almacenamiento de datos corporativo proporcionado comprende una copia del contenido originalmente almacenado verificado, limpiado y encriptado en el dispositivo de almacenamiento de datos privado. El método también comprende: en al menos uno de la pluralidad de dispositivos informáticos: detectar si un dispositivo de almacenamiento de datos insertado en un puerto del dispositivo informático es uno privado o uno corporativo; si es uno privado, denegar el acceso del dispositivo de almacenamiento de datos a ese dispositivo informático; y si es uno corporativo, comprobar si su contenido se ha verificado, limpiado y encriptado por un dispositivo de control y, en el caso en que lo haya sido, desencriptar el contenido del dispositivo de almacenamiento de datos, permitiendo por lo tanto que el dispositivo informático lea o ejecute ese contenido.

En una realización particular, la etapa de autenticación de usuario comprende leer una tarjeta de acceso o un identificador electrónico del usuario, en el que la lectura de la tarjeta o identificador electrónico se realiza insertando esa tarjeta en una ranura o detectando inalámbricamente la información registrada en la tarjeta o en el identificador electrónico; y la etapa de autenticación del dispositivo de almacenamiento de datos comprende comparar un identificador asociado al dispositivo de almacenamiento de datos con los identificadores comprendidos en una lista de identificadores que corresponden a respectivos dispositivos de almacenamiento de datos corporativos.

En una realización particular, el método comprende, después de autenticar el usuario y autenticar el dispositivo de almacenamiento de datos: copiar el contenido del dispositivo de almacenamiento de datos, en uno corporativo o en uno privado, en medio de memoria comprendido en el al menos un dispositivo de control; eliminar del contenido copiado cualquier software maligno; verificar que el contenido copiado pertenece a una lista de ficheros permitidos o extensiones de fichero permitidas; crear un fichero dentro del medio de memoria, comprendiendo ese fichero el

contenido sin software maligno que pertenece a la lista de ficheros permitidos; copiar el fichero creado en el dispositivo de almacenamiento de datos corporativo.

Más particularmente, antes de copiar el fichero creado en el dispositivo de almacenamiento de datos corporativo, el método realiza: encriptar simétricamente el fichero; hacer un troceo para comprobar su integridad; y firmar el fichero encriptado y troceado con una clave privada.

En una realización particular, la etapa de detección en al menos uno de la pluralidad de dispositivos informáticos si el dispositivo de almacenamiento de datos insertado en un puerto de dicho dispositivo informático es uno privado o uno corporativo comprende: comparar un identificador del dispositivo de almacenamiento de datos insertado con cada identificador de una lista de identificadores que corresponden a dispositivos de almacenamiento de datos corporativos.

El dispositivo de almacenamiento de datos puede ser una unidad de USB, o una mini unidad de USB, o una micro unidad de USB, o un DVD, o un CD, o una tarjeta SD, o una mini tarjeta SD o una micro tarjeta SD, o un disco duro portátil, o cualquier otro formato de sistema de almacenamiento de datos.

En una realización particular, el método comprende adicionalmente, en al menos uno de la pluralidad de dispositivos informáticos: enchufar en un puerto del al menos un dispositivo informático un adaptador que comprende un primer puerto configurado para recibir un dispositivo de almacenamiento de datos externo. El adaptador se enchufa en el puerto del dispositivo informático a través de un puerto del adaptador. El método también comprende enchufar en el primer puerto del adaptador un dispositivo de almacenamiento de datos externo; y proporcionar por el adaptador una interfaz física entre el dispositivo de almacenamiento de datos externo y el dispositivo informático mientras se aísla el dispositivo informático del dispositivo de almacenamiento de datos externo.

Más particularmente, el método comprende adicionalmente en el adaptador: detectar si el dispositivo de almacenamiento de datos insertado en el puerto del adaptador es uno privado o uno corporativo; si es uno privado, denegar el acceso del dispositivo de almacenamiento de datos a ese dispositivo informático; y si es uno corporativo, comprobar si su contenido se ha verificado, limpiado y encriptado por un dispositivo de control y, en el caso en que lo haya sido, desencriptar el contenido del dispositivo de almacenamiento de datos, permitiendo por lo tanto que el dispositivo informático lea o ejecute ese contenido. Se harán evidentes ventajas y características adicionales de la invención a partir de la descripción detallada que sigue y que se señalarán particularmente en las reivindicaciones adjuntas.

Breve descripción de los dibujos

Para completar la descripción y para proporcionar para un mejor entendimiento de la invención, se proporciona un conjunto de dibujos. Dichos dibujos forman una parte integral de la descripción e ilustran una realización de la invención, que no debería interpretarse como que restringe el alcance de la invención, sino solo como un ejemplo de cómo puede llevarse a cabo la invención. Los dibujos comprenden las siguientes figuras:

La Figura 1 muestra un esquema de la arquitectura del sistema de seguridad de acuerdo con una realización de la invención

Las Figuras 2A y 2B muestran dos vistas de un esquema de un dispositivo de control de acuerdo con una realización particular de la invención.

La Figura 3 muestra un esquema de la arquitectura de un adaptador de acuerdo con una posible realización de la invención

La Figura 4 muestra un diagrama de flujo de un proceso llevado a cabo en un adaptador de acuerdo con la invención antes de permitir que el contenido de un dispositivo de almacenamiento de datos externo se ejecute en un dispositivo crítico.

Las Figuras 5 a 10 muestran diferentes etapas de la arquitectura de un adaptador de acuerdo con una posible realización de la invención.

Descripción de una manera para llevar a cabo la invención

En este texto, el término “comprende” y sus derivaciones (tal como “que comprende”, etc.) no deben entenderse en un sentido excluyente, es decir, estas expresiones no deben interpretarse como que excluyen la posibilidad de lo que se describa y defina pueda incluir elementos, etapas adicionales, etc.

En el contexto de la presente invención, el término “aproximadamente” y términos de su familia (tal como “aproximado”, etc.) deben entenderse como que indican valores muy cercanos a aquellos que acompañan el término anteriormente mencionado. Es decir, debería aceptarse una desviación dentro de límites razonables de un valor

exacto, puesto que un experto en la materia entenderá que una desviación de este tipo de los valores indicados es inevitable debido a imprecisiones de medición, etc. Lo mismo se aplica a los términos “acerca de” y “alrededor” y “sustancialmente”.

La siguiente descripción no ha de tomarse en un sentido limitante sino que se proporciona solamente para el fin de describir los principios amplios de la invención. A continuación se describirán realizaciones de la invención a modo de ejemplo, con referencia a los dibujos anteriormente mencionados que muestran aparatos y resultados de acuerdo con la invención.

La Figura 1 muestra un esquema de la arquitectura de un sistema de seguridad 1 de acuerdo con una realización de la invención. El sistema de seguridad está asociado a un área industrial que tiene ordenadores o estaciones de trabajo (dispositivos industriales) de operación/control geográficamente dispersados 41 42 43 44 que forman un sistema crítico 400. Un sistema crítico es un sistema que abarca ordenadores, estaciones de trabajo y/u otros dispositivos cuyo fallo puede provocar daño grave, tal como lesión o muerte a seres humanos. Tales sistemas normalmente controlan un proceso en el mundo físico. El sistema de seguridad 1 comprende una pluralidad de puntos de comprobación, los dispositivos de control o dispositivos de acceso 11 12 13 (en lo sucesivo denominados como dispositivos de control) que sirven como puntos de entrada al área industrial que comprende ese sistema crítico 400. Los dispositivos de control 11 12 13 son dispositivos o aparatos en los que los empleados o visitantes del área (por ejemplo, sistema industrial) deben identificarse a sí mismos y registrar cualesquiera sistemas de almacenamiento de datos externos que planeen usar dentro de la instalación industrial. Ejemplos no limitantes de sistemas de almacenamiento de datos externos son cualquier sistema de almacenamiento de datos de entrada/salida, tal como unidades de USB, tal como unidades de USB, mini unidades de USB o micro unidades de USB, DVD, CD, tarjetas SD (Secure Digital), tal como mini tarjetas SD o micro tarjetas SD, discos duros portátiles o cualquier otro formato de sistema de almacenamiento de datos que pudiera plantear cualquier corpúsculo de almacenamiento digital. Los sistemas de almacenamiento de datos externos pueden no estar únicamente de manera potencial enchufados en los ordenadores que forman el sistema crítico 400, sino que también pueden insertarse en otros dispositivos electrónicos, tal como teléfonos inteligentes, relojes inteligentes, cámaras fotográficas, cámaras de vídeo, entre otros. Un servidor (no mostrado) controla la totalidad del sistema. El sistema de seguridad se gestiona por un usuario final que eventualmente gestiona las alertas de operación.

En una realización particular, el dispositivo de control 11 12 13 es un gabinete o caja, por ejemplo como se ilustra en las Figuras 2A y 2B El dispositivo de control 11 12 13 comprende medios informáticos que incluyen medios de memoria y medios de procesamiento configurados para, entre otras funcionalidades, autenticar usuarios (visitantes, empleados...), detectar software maligno y limpiar ficheros de software maligno. La autenticación puede realizarse leyendo una tarjeta de acceso o tarjeta de empleado (los visitantes normalmente llevan una tarjeta de acceso de visitante, mientras que los empleados llevan una tarjeta de empleado corporativo o tarjeta de id) o cualquier otro identificador electrónico llevado por un dispositivo asociado al usuario, tal como un teléfono inteligente, una PDA o un reloj. La autenticación puede realizarse de cualquier manera convencional, tal escribiendo un nombre de usuario y contraseña o insertando una tarjeta (tarjeta de acceso o tarjeta de id) en una ranura o mediante detección inalámbrica de la información registrada en la tarjeta o dispositivo que lleva un identificador electrónico. Para este fin, el dispositivo de control 11 12 13 comprende medios 112 para autenticación, tal como un sistema de NFC (Comunicación de Campo Cercano), ilustrado en la implementación ejemplar de la Figura 2A, a través del cual el usuario puede identificarse acercando una tarjeta de ID o dispositivo que lleva un identificador electrónico al sistema de NFC. El dispositivo de control 11 12 13 está equipado con una pluralidad de diferentes puertos, cada uno configurado para recibir un sistema de almacenamiento de datos diferente, tal como los ya enumerados, la Figura 2A muestra dos puertos a modo de ejemplo, ambos denominados en general como 111, configurados para recibir respectivos diferentes tipos de sistemas o dispositivos de almacenamiento de datos. Como se explicará más adelante, a través de uno de estos puertos 111, una vez autenticado el usuario puede insertar el sistema de almacenamiento de datos que planea usar dentro de la instalación industrial en un correspondiente puerto 111. Por ejemplo, se solicita que un usuario (por el sistema de seguridad) inserte tal sistema de almacenamiento de datos visualizando un mensaje en una pantalla visual 110 o emitiendo una señal audible o por altavoz (no ilustrado). En una realización particular, el sistema de almacenamiento de datos es una unidad de USB. El dispositivo de control 11 12 13 también comprende medios 113 para expedir un dispositivo de almacenamiento de datos corporativo. En una realización particular, el dispositivo de almacenamiento de datos corporativo es una unidad de USB flash corporativa. Cuando el dispositivo de almacenamiento de datos que el usuario (es decir visitante o empleado) pretende usar dentro de la instalación industrial es uno privado (a diferencia de uno corporativo), el dispositivo de control 11 12 13, después de una etapa de verificación de software y limpieza que se explicará en detalle más adelante, proporciona al usuario con un dispositivo de almacenamiento de datos corporativo, sin software maligno ni software no permitido.

El dispositivo de control 11 12 13 tiene medios de verificación configurados para verificar que el software (datos en general) almacenado en el sistema de almacenamiento de datos está limpio y sin software maligno. El posible software maligno o las infecciones se limpiarán. A continuación, se prepara por el sistema un dispositivo de almacenamiento de datos corporativo (en una realización particular, una unidad de USB o unidad de USB flash), alojado en el dispositivo de control 11 12 13. El dispositivo de almacenamiento de datos corporativo únicamente contiene el software verificado y los datos (software y datos limpiados) del dispositivo de almacenamiento de datos

externo original. Este dispositivo de almacenamiento de datos corporativo o interno está vinculado o asociado a su portador a través de una identificación del usuario ya extraída en la etapa de autenticación. Una vez que se autentica el usuario, el ID único de ese usuario está vinculado al ID del USB corporativo proporcionado por el dispositivo de control 11 12 13. Los contenidos de este dispositivo de almacenamiento de datos corporativo se encriptan tanto asimétrica como simétricamente. En suma, se realizan mecanismos de autenticación y autorización para poder garantizar un correcto control de acceso. Estos mecanismos se explican en detalle más adelante en esta descripción.

Para conseguir una solución de seguridad coherente y distribuida, el sistema de seguridad 1 también comprende una pluralidad de agentes de software 20 instalados en los dispositivos críticos (sistemas informáticos o dispositivos informáticos) 41 42 43 44 y/o en adaptadores (dispositivos de interfaz) 30 (que van a describirse), que son dispositivos que comprenden agentes de software. Un agente de software es software instalado en un dispositivo o estación de trabajo para proteger ese dispositivo o estación de trabajo contra dispositivos de almacenamiento de datos no autorizados, tal como unidades de USB. El software comprendido en el agente de software es un programa de SO nativo que deniega la operación de dispositivos de almacenamiento de datos (tal como la operación USB) a menos que estos dispositivos de almacenamiento de datos se reconozcan por la corporación. Los agentes de software 20 y los adaptadores 30 se despliegan en los dispositivos industriales 41 42 43 44 comprendidos en la planta industrial. Estos agentes y/o adaptadores controlan y aseguran que únicamente los dispositivos de almacenamiento de datos corporativos, tal como unidades de USB corporativas, encriptadas por un dispositivo de control determinado 11 12 13 y vinculadas a un portador registrado específico, como se explicará a continuación, tendrán acceso a dispositivos críticos 41 42 43 44 en el sistema de operación industrial.

El área de la instalación industrial cubierta por el sistema de seguridad 1, es decir, el área que tiene dispositivos críticos (sistemas informáticos) 41 42 43 44 que están controlados/protegidos por los dispositivos de control 11 12 13 y los agentes de software 20 y/o adaptadores 30 asociados a los dispositivos críticos 41 42 43 44, se denomina “zona desinfectada” o “zona blanca”, en el sentido que esta zona está sin software maligno originado en los sistemas de almacenamiento de datos externos. En otras palabras, una “zona blanca” es un área lógica que está sin virus o código ejecutable malicioso que proviene de dispositivos de almacenamiento de datos en un área física particular. Esta área puede abarcar varios dispositivos críticos y estaciones de trabajo dentro de ella. Los empleados y visitantes que acceden a esta zona necesitan asumir reglas particulares para operar dentro de la planta industrial. Los empleados y visitantes acceden a esta zona después de identificarse a sí mismos y realizar algunas tareas de seguridad en un dispositivo de control 11 12 13, como se explicará a continuación.

A continuación, se describen en detalle las acciones a realizarse en un dispositivo de control 11 12 13 cuando un usuario desea acceder a una “zona blanca” con un dispositivo de almacenamiento de datos externo (con la intención de insertar/leer/copiar/ejecutar el dispositivo de almacenamiento de datos externo en un dispositivo crítico 41 42 43 44). Como ya se ha indicado, un dispositivo de control 11 12 13 es un dispositivo o aparato que tiene como objetivo limpiar un dispositivo de almacenamiento de datos externo en términos de virus de software y software maligno y verificar que únicamente software válido (software incluido en una “lista blanca”) proviene de un dispositivo de almacenamiento de datos externo está permitido a entrar en una “zona blanca”. Tienen que realizarse un conjunto de etapas o pasos en el dispositivo de control 11 12 13.

En primer lugar, se requiere una etapa de autenticación/verificación. El dispositivo de control 11 12 13 comprende medios para autenticar usuarios (visitantes, empleados ...). Esta autenticación está basada en medios de software. Un usuario se autentica con el sistema (en un dispositivo de control 11 12 13) por medio de cualquier proceso de autenticación. La autenticación puede realizarse escribiendo el nombre de usuario/contraseña o leyendo una tarjeta de acceso o tarjeta de empleado o cualquier otro identificador electrónico llevado o integrado en un dispositivo portátil (teléfono inteligente, reloj inteligente, PDA …) en los medios para autenticación 112 comprendidos en el dispositivo de control 11 12 13 (los visitantes normalmente llevan una tarjeta de acceso de visitante, mientras que los empleados llevan una tarjeta de empleado corporativo o tarjeta de id o un identificador electrónico diferente como ya se ha mencionado). La autenticación puede realizarse de cualquier manera convencional, tal como a través de un método de autenticación de usuario/contraseña básico (por ejemplo para escribirse por el usuario en una pantalla táctil o teclado), o por medio de una tarjeta de ID o tarjeta de acceso o identificador electrónico (ya sea insertándola en una ranura o por detección inalámbrica de la información registrada en la tarjeta o identificador electrónico). En particular los entornos o escenarios que implican requisitos de seguridad máxima, la etapa de autenticación realizada por el dispositivo de control 11 12 13 implica autenticación de dos factores. La autenticación de dos factores es un proceso de seguridad en el que el usuario proporciona dos medios de identificación, uno de los cuales es normalmente un testigo físico, tal como una tarjeta de ID o identificador electrónico, y el otro es normalmente algo memorizado, tal como un nombre de usuario/contraseña. En otras palabras, la autenticación de dos factores implica una combinación de lectura de un testigo de acceso más escritura de una clase de código. Un ejemplo no limitante de tecnología actual para transmitir el testigo de posesión de autenticación (tal como tarjeta de id o tarjeta de empleado o identificador electrónico) es mediante NFC (Comunicación de Campo Cercano). En la realización ilustrada en la Figura 2A, el dispositivo de control 11 12 13 preferentemente comprende un lector de NFC. El lector de NFC obtiene un identificador único (tal como el UUID (identificador universalmente único)) de la tarjeta de id o identificador electrónico y lo envía a un servidor 50 (no ilustrado), en el que el usuario se autentica contra un directorio. El directorio puede ser una base de datos local o un servidor de LDAP (Protocolo Ligero de Acceso al

Directorio).
Esta etapa de autenticación requiere también que el dispositivo de almacenamiento de datos externo llevado por el usuario se autentique también. El dispositivo de almacenamiento de datos externo llevado por el usuario se enchufa a continuación en un puerto o ranura correspondiente del dispositivo de control 11 12 13. En una realización particular, el dispositivo de almacenamiento de datos externo está incorporado en la tarjeta (es decir tarjeta de empleado) o dispositivo que lleva un identificador electrónico. En este caso, el dispositivo de almacenamiento de datos externo es uno corporativo. En una situación más general, el dispositivo de almacenamiento de datos externo llevado por el usuario puede ser cualquiera de un dispositivo de almacenamiento de datos corporativo (por ejemplo puesto que el usuario es un empleado) o un dispositivo de almacenamiento de datos no corporativo (es decir, un dispositivo privado de propiedad por cualquiera de un visitante o un empleado). Para realizar esta autenticación del dispositivo de almacenamiento de datos externo, el identificador único (por ejemplo UUID) del dispositivo de almacenamiento de datos externo se compara con una lista de identificadores únicos que corresponden a respectivos dispositivos de almacenamiento corporativos. Esta comparación puede realizarse localmente (en el dispositivo de control 11 12 13) o de manera remota (en el servidor 50). Posteriormente, hay tres posibles escenarios:

(1) Si el dispositivo de almacenamiento de datos externo es uno corporativo (y por lo tanto su identificador único se ha hecho coincidir correctamente con uno de la lista de dispositivos de almacenamiento de datos corporativos), el dispositivo de control 11 12 13 no expedirá uno corporativo puesto que el usuario ya tiene uno. El dispositivo de control 11 12 13 realizará, sin embargo, varias tareas de seguridad que se explicarán a continuación (escenario 1).

(2) Si el dispositivo de almacenamiento de datos externo es uno no corporativo y el papel del usuario indica (esto puede indicarse por ejemplo durante la autenticación de usuario) que él está autorizado a proporcionársele con un USB corporativo, el dispositivo de control 11 12 13 proporcionará uno corporativo una vez que se han realizado tareas de seguridad adicionales en el software almacenado en el dispositivo de almacenamiento de datos externo, como se explicará a continuación (escenario 2).

(3) Si el dispositivo de almacenamiento de datos externo es uno no corporativo y el papel del usuario indica (preferentemente durante una etapa de autenticación) que él no está autorizado a proporcionársele un dispositivo de almacenamiento de datos corporativo, el dispositivo de control 11 12 13 no proporcionará uno corporativo y no se realizarán tareas de seguridad adicionales.

En ambos escenarios (1) y (2), una vez que el dispositivo de control 11 12 13 tiene conocimiento del hecho de que el dispositivo de almacenamiento de datos externo se enchufa, se hace lo siguiente. Preferentemente, se borra una carpeta de fichero temporal, normalmente usada para el procedimiento de limpieza en los medios informáticos del dispositivo de control. La carpeta de fichero temporal se borra preferentemente para crear una nueva en la que realizar las acciones de verificación de limpieza y software. A continuación, comienza un proceso de copia. Los ficheros del dispositivo de almacenamiento de datos externo (tal como la unidad de USB, ya sea una corporativa (escenario (1)) o una privada (escenario (2))) se copian a un fichero temporal nuevamente creado en la carpeta de fichero temporal en el dispositivo de control 11 12 13. Una vez copiados, estos ficheros se limpian por un antivirus externo de una manera convencional. En el contexto de la invención, “limpieza” significa que un servicio anti-software maligno limpia/elimina el software maligno dentro del conjunto de ficheros seleccionados (ficheros copiados del dispositivo de almacenamiento). Los procesos de detección y limpieza de tecnología de anti-software maligno convencionales se realizan usando firmas y patrones conocidos. Además de limpiar el fichero o software infectado, se lleva a cabo alguna verificación, en la que se verifica si los ficheros copiados pertenecen o están en una lista (“lista blanca”) que comprende ficheros correctos o permitidos de acuerdo con la política de seguridad de organización. Por ejemplo, la lista de ficheros permitidos puede comprender una lista exhaustiva de posibles extensiones permitidas para los ficheros. En otras palabras, la verificación es un proceso que posibilita la entrada de únicamente ficheros y aplicaciones bien conocidos. En una realización particular, los procesos de limpieza y verificación se realizan por un servicio en la nube. Una vez que se finalizan estos dos procesos (limpieza y verificación), todos los ficheros en la carpeta temporal se comprimen (es decir comprimidos en formato zip) en un único fichero comprimido (aún dentro de los medios de memoria comprendidos en el dispositivo de control) y se encriptan. El proceso de criptografía abarca estas etapas:

- el fichero comprendido (es decir el fichero zip) se encripta simétricamente con un secreto para mantener la confidencialidad;

- se realiza un troceo para comprobar su integridad y se firma con la clave privada del punto de comprobación (clave privada del dispositivo de control 11 12 13);

- una lista de dispositivos de almacenamiento de datos corporativos se encripta simétricamente con un secreto o frase de paso.

A continuación se inicia una segunda etapa. En el escenario (2), se proporciona un dispositivo de almacenamiento de datos corporativo por el dispositivo de control 11 12 13. El usuario a continuación monta (enchufa) el dispositivo

de almacenamiento de datos corporativo en un puerto del dispositivo de control 11 12 13 para copiar los ficheros previamente generados (almacenados en la carpeta de fichero temporal creada) más la clave pública del punto de comprobación (dispositivo de control 11 12 13). La generación de claves públicas y claves privadas está fuera del alcance de la presente invención. Los cuatro ficheros generados (contenido original encriptado, fichero de troceo encriptado, lista encriptada de dispositivos de almacenamiento de datos corporativos y clave pública) se copian al dispositivo de almacenamiento de datos corporativo. A continuación, en una realización preferida, una vez que se copian los cuatro ficheros en el dispositivo de almacenamiento de datos corporativo, la carpeta temporal en el dispositivo de control 11 12 13 se borra a través de un proceso de borrado seguro. Antes de copiar los cuatro ficheros en el dispositivo de almacenamiento de datos corporativo por el dispositivo de control 11 12 13, se realiza un borrado seguro del contenido almacenado anterior del dispositivo de almacenamiento de datos corporativo que va a proporcionarse en el dispositivo de control 11 12 13.

Después de este proceso, el dispositivo de almacenamiento de datos corporativo proporcionado por el dispositivo de control 11 12 13 comprende cuatro ficheros:

- un fichero que comprende el contenido comprimido y encriptado del dispositivo de almacenamiento de datos original insertado en el dispositivo de control 11 12 13 por el usuario;

- una lista encriptada de los números de serie de todos los dispositivos de almacenamiento de datos corporativos válidos dentro de la “zona blanca”; esta lista permitirá que un agente de software compruebe, cuando se inserta el dispositivo corporativo en un dispositivo crítico, si el dispositivo insertado es o no un dispositivo de almacenamiento de datos corporativo válido;

- un fichero firmado digital con el valor de troceo del contenido encriptado, para comprobar si el contenido creado por el dispositivo de control que proporcionó el dispositivo de almacenamiento de datos corporativo se ha modificado o no (integridad); y

- la clave pública necesaria para leer los datos firmados y verificar la integridad del contenido encriptado.

Una vez que se satisface este proceso en el dispositivo de control, el usuario (visitante, empleado...) puede usar los contenidos que se han transferido desde su dispositivo de almacenamiento de datos privado al corporativo, en cualquier dispositivo crítico (ordenador...) que pertenezca a la “zona blanca”.

En el escenario (1), en el que el usuario lleva consigo un dispositivo de almacenamiento de datos corporativo, el dispositivo de control 11 12 13 no proporciona un dispositivo de almacenamiento de datos corporativo. Los cuatro ficheros generados (contenido original encriptado, fichero de troceo encriptado, lista encriptada de dispositivos de almacenamiento de datos corporativos y clave pública) almacenados en una carpeta temporal en el dispositivo de control 11 12 13 se copian al dispositivo de almacenamiento de datos corporativo. A continuación, en una realización preferida, una vez que se copian los cuatro ficheros en el dispositivo de almacenamiento de datos corporativo, la carpeta temporal en el dispositivo de control 11 12 13 se borra a través de un proceso de borrado seguro. Antes de copiar los cuatro ficheros en el dispositivo de almacenamiento de datos corporativo por el dispositivo de control 11 12 13, se realiza un borrado seguro del contenido almacenado anterior del dispositivo de almacenamiento de datos corporativo que va a proporcionarse en el dispositivo de control 11 12 13.

Después de este proceso en el escenario (1), el dispositivo de almacenamiento de datos corporativo llevado por el usuario tiene los mismos contenidos como se describe en escenario (2).

Una vez que se satisface este proceso en el dispositivo de control, el usuario (visitante, empleado...) puede usar los contenidos almacenados en el dispositivo de almacenamiento de datos corporativo, en cualquier dispositivo crítico (ordenador...) que pertenece a la “zona blanca”.

En la “zona blanca” (que comprende dispositivos críticos 41 42 43 44) en la instalación industrial, puede haber dos tipos de los dispositivos críticos o estaciones críticas: un primer tipo de dispositivos en los que se permite conectar en dispositivos de almacenamiento de datos externos (a los que se hace referencia en la Figura 1 como 41 42); en este primer tipo de dispositivos 41 42 se permite instalar software con la condición de que se hayan satisfecho ya los requisitos de seguridad; y un segundo tipo de dispositivos en los que está absolutamente prohibido enchufar cualquier dispositivo de almacenamiento de datos externo (excepto los adaptadores ya mencionados 30, que están autorizados puesto que pertenecen al sistema de seguridad 1). Este segundo tipo de dispositivos se hace referencia en la Figura 1 como 43 44. En este segundo tipo de dispositivos críticos 43 44 está totalmente prohibido instalar software.

En particular, un usuario dentro de una “zona blanca” puede llevar un dispositivo de almacenamiento de datos (es decir unidad de USB) y ese dispositivo de almacenamiento de datos puede ser un dispositivo de almacenamiento de datos corporativo o un dispositivo de almacenamiento de datos privado. Cuando el usuario inserta el dispositivo de almacenamiento de datos en un puerto adecuado de un dispositivo crítico (es decir estación de trabajo) 41 42 del primer tipo, un agente de software 20 instalado en ese dispositivo crítico (dispositivo informático) identifica un

identificador del dispositivo de almacenamiento de datos (por ejemplo, su UUID o su número de serie) y compara el identificador único del dispositivo de almacenamiento de datos con una lista de identificadores permitidos. El agente de software 20 tiene acceso a la lista de identificadores permitidos, ya sea puesto que tiene una conexión remota con el servidor 50 (por ejemplo una conexión de internet mediante web) o comprobando la lista almacenada en un fichero en el dispositivo de almacenamiento de datos. Si el dispositivo de almacenamiento de datos es uno privado, la comparación no coincide con ningún identificador en la lista. El dispositivo de almacenamiento de datos privado se rechaza automáticamente del dispositivo crítico 41 42. Cualquier software maligno de arranque que pudiera instalarse potencialmente en el dispositivo de almacenamiento de datos no puede alcanzar/ejecutarse/marchar en el dispositivo crítico 41 42.

Si, por el contrario, el dispositivo de almacenamiento de datos es uno corporativo (proporcionado por un dispositivo de control), la comparación del identificador del dispositivo externo coincide con un identificador en la lista. Esto se hace de una manera inversa con respecto al proceso llevado a cabo en el punto de comprobación:

- la clave pública se extrae del dispositivo de almacenamiento de datos y se verifica si se ha firmado o no el contenido por el dispositivo de control. Por lo tanto también se confirma que ese contenido se ha verificado por el dispositivo de control;

- la integridad se comprueba completando un algoritmo de función de troceo. Esto significa que el troceo inverso ha de corregirse para proporcionar luz verde para continuar con el proceso;

- el fichero con el contenido original se desencripta y se descomprime del formato zip;

- si todas las etapas previas son correctas, se abre una distribución/ventana en un visor/pantalla comprendida en el dispositivo crítico 41 42, que muestra el contenido del dispositivo de almacenamiento de datos corporativo;

- si una de las etapas anteriores no es válida, el dispositivo de almacenamiento de datos corporativo se rechaza automáticamente del dispositivo crítico 41 42.

Cuando el usuario desea insertar un dispositivo de almacenamiento de datos en un puerto adecuado 436 de un dispositivo crítico (es decir estación de trabajo) 43 44 del segundo tipo, es decir, un dispositivo crítico en el que está prohibido totalmente instalar/conectar/enchufar cualquier dispositivo de almacenamiento de datos externo, se requiere un adaptador, dispositivo de interfaz o dispositivo de almacenamiento de datos inteligente 30. De ahora en adelante en este texto, el término “adaptador” se usa hacer referencia a tal dispositivo 30. El adaptador 30 es el único dispositivo de almacenamiento de datos que se permite que se conecte en un puerto del dispositivo crítico.

El adaptador 30 es un dispositivo externo que va a enchufarse en un dispositivo crítico 43 44 del segundo tipo. En su apariencia exterior, el adaptador 30 comprende un primer puerto o enchufe 31 configurado para recibir un correspondiente dispositivo de almacenamiento de datos externo (es decir, un dispositivo de almacenamiento de datos externo del tipo adecuado para insertarse en dicho puerto o enchufe 31) y un segundo puerto o enchufe 32 configurado para enchufarse en un correspondiente puerto 436 del dispositivo crítico 43 44. En una implementación particular, los puertos o enchufes son puertos o enchufes USB, es decir, configurados para recibir/enchufar (según el caso pueda ser) una unidad de USB. En este caso, el adaptador 30 puede considerarse una unidad de USB inteligente. En suma, el adaptador 30 tiene una entrada física (el enchufe o puerto 31) y una salida física (enchufe o puerto 32) configuradas para conectarse a un correspondiente puerto 436 de un dispositivo crítico, al que han de transferirse los datos. En otras palabras, el adaptador 30 permite que un usuario enchufe un dispositivo de almacenamiento de datos externo en el primer puerto 31 y, puesto que el segundo puerto 32 del adaptador 30 se enchufa en el correspondiente puerto 436 del dispositivo crítico, la verificación de software puede hacerse en el adaptador 30, que comprende preferentemente un agente de software similar al agente de software 20 instalado en los dispositivos críticos 41 42 del primer tipo, manteniendo por lo tanto el dispositivo crítico 43 44 aislado del dispositivo de almacenamiento de datos externo. En resumen, el adaptador 30 que es una unidad de sistema de almacenamiento de datos inteligente, está conectado como una unidad de sistema de almacenamiento de datos y se comporta como una unidad de sistema de almacenamiento de datos. La Figura 3 muestra un esquema de la arquitectura de un adaptador 30 de acuerdo con una posible realización de la invención. A continuación, se explica cómo funciona esto.

El adaptador 30 comprende hardware y componentes o elementos de software. Comprende los siguientes componentes funcionales: medios de control 33, medios de almacenamiento de datos internos 34 y medios de aislamiento o medios de conmutación 35.

El medio de control 33 es un componente funcional asociado a varios elementos de hardware, tal como al menos un microprocesador o una CPU 331 y al menos una memoria 332 (esta al menos una memoria 332 puede implementarse, por ejemplo, por medio de una memoria volátil y una memoria permanente). El medio de control 33 puede implementarse por ejemplo como cualquier dispositivo similar a ordenador, tal como una caja de pc o un microordenador. Comprende un sistema operativo y una aplicación de software configurados para controlar la información para pasarse a una máquina externa o máquina de destino (dispositivo crítico 43 44). Los medios de

almacenamiento de datos internos 34 (también denominados como medios de almacenamiento de datos auxiliares) pueden ser cualquier sistema de almacenamiento de datos, tal como una unidad de USB, mini unidad de USB, unidad de micro USB, tarjeta SD (Secure Digital), tarjeta mini SD o tarjeta micro SD. En una realización preferida, es una unidad de USB. El adaptador 30 también comprende un puerto o enchufe interno 36 configurado para recibir el medio de almacenamiento de datos interno 34 en el ejemplo particular en el que el medio de almacenamiento de datos interno 34 es una unidad de USB, el puerto o enchufe interno 36 es un puerto o enchufe USB. El medio de almacenamiento de datos interno 34 es el único enlace entre los medios de control 33 y el dispositivo crítico 43 44 a protegerse. Como se explicará más adelante, el medio de almacenamiento de datos interno 34 puede conectarse (indirectamente), mediante software, al dispositivo crítico 43 44 y al adaptador 30. La única conexión entre el adaptador 30 y el dispositivo crítico 43 44 es la salida física 32 del adaptador (enchufe o puerto 32).

Los medios de aislamiento o medios de conmutación 35 son un componente funcional asociado a varios componentes electrónicos que posibilitan la realización de una conexión entre el medio de almacenamiento de datos interno 34, los medios de control 33 y el dispositivo crítico externo 43 44 al que está enchufado físicamente el adaptador 30 a través del enchufe o puerto 32. Como se muestra en la Figura 3 mediante la línea que conecta los medios de aislamiento 35 y el enchufe 36, el medio de almacenamiento de datos interno 34 está únicamente conectado a los medios de aislamiento 35, que es el elemento funcional que permite la conexión lógica entre el medio de almacenamiento de datos interno 34 y cualquier otro elemento. Esta conexión lógica se permite por los medios de aislamiento o medios de conmutación 35 pero se controla y gestiona por los medios de control 33. En otras palabras, los medios de aislamiento o conmutación 35 son o actúan como un conmutador configurado para aislar o comunicar otros elementos que siguen las instrucciones de los medios de control 33. La operación del adaptador 30 se explica en detalle en relación a la Figura 4.

Como ya se ha mencionado, el adaptador 30 se pretende que se enchufe en un correspondiente puerto 436 de un dispositivo crítico 43 44. Ejemplos no limitantes de dispositivos críticos son: un ordenador personal, un portátil, un PLC (controlador de lógica programable), un sistema SCADA, entre otros. Conectando el adaptador 30 al dispositivo crítico 43 44. El dispositivo crítico únicamente intercambia datos con el dispositivo de almacenamiento de datos interno (dispositivo de almacenamiento de datos auxiliar) 34. El adaptador 30 funciona por lo tanto como una interfaz entre un dispositivo de almacenamiento de datos externo (insertado en el primer enchufe o puerto 31 del adaptador 30) llevado por un usuario y el dispositivo crítico 43 44 en el que los datos almacenados en el dispositivo de almacenamiento de datos externo se pretende que se carguen/ejecuten. Estos datos comprendidos en el dispositivo de almacenamiento de datos externo llevado por el usuario se validan (o no, según el caso pueda ser) en el adaptador 30 (en particular, en los medios de control 33) y, si la validación es correcta, los ficheros permitidos se transfieren al dispositivo de almacenamiento de datos interno (auxiliar) 34 comprendido en el adaptador 30.

A continuación se proporciona una descripción funcional en relación con el gráfico de flujo de la Figura 4 y varias etapas del adaptador 30 representadas en las Figuras 5-10. El adaptador 30 está conectado por defecto (por medio del puerto o el enchufe 32) a un puerto correspondiente 436 de un dispositivo crítico 43 44 (en el que no se permite que se conecte ningún otro (diferente del adaptador) dispositivo de almacenamiento de datos externo. El puerto 436 está bloqueado física y permanentemente por el adaptador 30. Por lo tanto, no es posible otra conexión física en el puerto 436. Cuando no está conectado el dispositivo de almacenamiento de datos externo (por medio del puerto o enchufe 31) al adaptador 30, el adaptador 30 mantiene una conexión lógica entre la unidad de almacenamiento de datos interna (auxiliar) 34 y el dispositivo crítico 43 44. Esta conexión “ficticia” entre la unidad o medios de almacenamiento de datos interno 34 y el dispositivo crítico 43 44 se requiere puesto que el dispositivo crítico únicamente entiende el adaptador 30 como un dispositivo de almacenamiento de datos y no como cualquier otro componente que requiere por ejemplo la instalación de software, controladores, etc. Preferentemente, para mejorar la seguridad, todos los enchufes o puertos de entrada/salida del dispositivo crítico 43 44 se desactivan o bloquean, de modo que el único punto de entrada de datos/ficheros es mediante el adaptador 30.

Haciendo referencia a la Figura 4, en una etapa inicial (“Inicio”, etapa 400) el adaptador 30 está en un estado inicial que puede hacerse referencia como un estado “en espera”. Este estado inicial o estado en espera del adaptador 30 se representa en la Figura 5. Las Figuras 5-10 representan diferentes etapas del adaptador 30. En línea en negrita o línea gruesa mostramos los componentes que están directa o indirectamente conectados al dispositivo de almacenamiento de datos interno 34 en cada etapa. En línea discontinua, mostramos los componentes activos en cada etapa de proceso aparte de los que están directa o indirectamente conectados al dispositivo de almacenamiento de datos interno 34.

El estado inicial implica que el adaptador 30 está activado (en un estado “ACTIVADO”) y el enchufe o puerto 32 se enchufa en un correspondiente puerto o enchufe 436 de un dispositivo crítico 43 44. El dispositivo de almacenamiento de datos interno (dispositivo de almacenamiento de datos auxiliar) 34 está conectado al dispositivo crítico (y no a cualquier dispositivo o parte del adaptador 30). El dispositivo de almacenamiento de datos interno 34 está siempre conectado en un enchufe interno 36. El adaptador 30 aísla el dispositivo crítico 43 44 de cualquier medio de almacenamiento de datos externo (denominado como 61 en la Figura 6) y los medios de almacenamiento de datos externos no están física y directamente conectados al dispositivo crítico 43 44. Los medios de aislamiento 35 posibilitan la conexión lógica entre el dispositivo de almacenamiento de datos interno 34 y el dispositivo crítico 43 44. Esta conexión lógica está permitida por los medios de aislamiento o conmutación 35 pero controlada y

gestionada por los medios de control 33. En este estado por defecto (estado “en espera”), se establece una conexión “ficticia” entre la unidad o medios de almacenamiento de datos interno 34 y el dispositivo crítico 43 44. De esta manera, el dispositivo crítico 43 44 entiende que el adaptador 30 es un dispositivo de almacenamiento de datos. Gracias a esta conexión lógica, el dispositivo crítico 43 44 puede leer o detectar, por ejemplo en una aplicación para exploración de fichero, el dispositivo de almacenamiento de datos interno 34 como si este dispositivo 34 estuviera físicamente enchufado en el puerto 436 del dispositivo crítico 43 44. Por el contrario, el dispositivo crítico 43 44 no puede leer o detectar el adaptador 30 (como una totalidad). En otras palabras, para el dispositivo crítico, el adaptador 30 no existe. Para el dispositivo crítico, únicamente existe un dispositivo de almacenamiento de datos (en esta etapa, el dispositivo de almacenamiento de datos interno 34). Como consecuencia, no hay necesidad de instalar ningún controlador específico o software en el dispositivo crítico. Se destaca que hasta ahora, no hay dispositivo de almacenamiento de datos externo enchufado en el puerto o enchufe 31 del adaptador 30.

El proceso se inicia cuando un dispositivo de almacenamiento de datos externo 61 con contenido protegido 615 (por el dispositivo de control 11 12 13) llevado por un usuario se inserta en el adaptador 30 mediante el puerto 31 (etapa 401). Este dispositivo de almacenamiento de datos externo 61 puede ser cualquier dispositivo de almacenamiento de datos, por ejemplo uno corporativo o uno privado. Cuando se inserta el dispositivo externo 61, los medios de control 33 (microprocesador o CPU 331 y la memoria 332) detectan este evento y empiezan a recopilar información del dispositivo externo 61. Hasta ahora, no se conmuta la conexión. Esto significa que mientras que los medios de control 33 interrogan el dispositivo de almacenamiento de datos externo 61, el dispositivo de almacenamiento de datos interno 34 sigue estando conectado lógicamente al puerto o enchufe 436 del dispositivo crítico 43 44.

A continuación, se ejecuta una verificación del dispositivo de almacenamiento de datos externo 61 (etapa 402), para determinar si ese dispositivo de almacenamiento de datos externo 61 es uno autorizado (uno válido) o no. En una realización particular, los dispositivos externos autorizados 61 son aquellos dispositivos externos que son corporativos y se proporcionan por dispositivos de control 11 12 13. En este caso, el proceso de verificación es preferentemente el mismo proceso de verificación que ya se ha descrito con respecto al agente de software.

Si ese dispositivo externo 61 no es uno válido, no se ejecutan operaciones adicionales. Si el dispositivo externo 61 es válido, se ejecuta verificación adicional (etapa 403), para comprobar si los ficheros almacenados en el dispositivo externo 61 son ficheros válidos (permitidos). En la Figura 6, los ficheros 615 almacenados en el dispositivo externo 61 están esquematizados. Este contenido se examina por los medios de control 33. Preferentemente, este proceso de verificación de fichero es el mismo proceso de verificación de fichero que ya se ha descrito con respecto al agente de software, es decir, se verifica si su contenido no se ha modificado desde la última vez que se verificó por un dispositivo de control 11 12 13. Si esta operación no es satisfactoria, el adaptador 30 interrumpe cualquier acción asociada al dispositivo de almacenamiento de datos externo 61 y vuelve al estado inicial (estado en espera). Este proceso se determina de esta manera. Si, por el contrario, la operación es satisfactoria, implica que los ficheros 615 son válidos. En la Figura 6, los componentes activos implicados en la verificación del dispositivo externo 61 y su contenido 615 se muestran en línea discontinua.

En otras palabras, el adaptador 30 comprende medios para detectar si el dispositivo de almacenamiento de datos 61 insertando en el puerto 31 del adaptador 30 es uno privado o uno corporativo. En el caso de un privado, deniega el acceso del dispositivo de almacenamiento de datos a ese dispositivo informático 43 44. En el caso de uno corporativo, comprueba si su contenido se ha verificado y limpiado por un dispositivo de control 11 12 13 y, en el caso en que lo haya sido, desencripta el contenido del dispositivo de almacenamiento de datos, permitiendo por lo tanto que el dispositivo informático crítico 43 44 lea o ejecute dicho contenido.

En el caso que todas las validaciones (etapas 402, 403) sean satisfactorias, el adaptador 30 desconecta el medio de almacenamiento de datos interno 34 de la conexión por defecto lógica al dispositivo crítico (destacado en línea en negrita en la Figura 5) y conecta lógicamente el medio de almacenamiento de datos interno 34 al adaptador 30 (en particular, a los medios de control 33) (etapa 404). Esto se ilustra en la Figura 7. Esto está controlado por los medios de control 33, que son responsables de cambiar el estado de los medios de aislamiento 35 de manera que las conexiones lógicas del dispositivo de almacenamiento de datos interno 34 están cambiadas (desconectando la conexión entre el dispositivo de almacenamiento de datos interno y el dispositivo crítico). Esto implica que el dispositivo crítico 43 44 deja de detectar o leer el dispositivo de almacenamiento de datos interno 34. El estado del dispositivo de almacenamiento de datos interno 34 con respecto al dispositivo crítico 43 44 es como si el dispositivo de almacenamiento de datos interno 34 se hubiera desenchufado físicamente del dispositivo crítico 43 44. Sin embargo, no se ha realizado manipulación física. Los medios de control 33 ahora detectan o leen el dispositivo de almacenamiento de datos interno 34. Preferentemente, la unidad de almacenamiento de datos interna 34 se limpia (su contenido se borra) para evitar que el adaptador 30 se contamine con contenido indeseado, virus, etc.

Ahora, los datos 615 almacenados en el dispositivo de almacenamiento de datos externo 61 llevado por el usuario pueden desencriptarse de manera segura y transferirse del dispositivo de almacenamiento de datos externo 61 al medio de almacenamiento de datos interno 34 (etapa 405) (datos 615b en la Figura 8), mientras que los enchufes de entrada/salida del dispositivo crítico 43 44 están aún bloqueados. Esto se hace como sigue: el fichero o ficheros 615 almacenados en el dispositivo de almacenamiento de datos externo 61 se copian en un fichero temporal 615a localizado en o creado en los medios de memoria 332. El fichero o ficheros copiados 615a es/están entonces

desencriptados, preferentemente de una manera similar a medida que los ficheros se desencriptan por un agente de software como se ha descrito anteriormente. Los ficheros desencriptados 615a se copian de los medios de memoria 332 en el medio de almacenamiento de datos interno 34 (ficheros desencriptados ahora referenciados como 615b en el dispositivo de almacenamiento de datos interno 34). El fichero o ficheros copiados en los medios de memoria 332 se borran. Esta etapa se ilustra en la Figura 8, en la que la conexión entre el dispositivo de almacenamiento de datos interno 34 y el dispositivo crítico 43 44 ya no está más en negrita. Se destaca que la conexión entre los medios de memoria 332 y los medios de aislamiento 35 ahora está en negrita, que significa que hay una conexión entre los medios de memoria 332 y el dispositivo de almacenamiento de datos interno 34.

Finalmente (etapa 406), los medios de control 33 desconectan el medio de almacenamiento de datos interno 34 del adaptador 30 y conectan el medio de almacenamiento de datos interno 34 al dispositivo crítico 43 44. Esto se ilustra en la Figura 9, que destaca de nuevo (en negrita) la conexión entre los medios de aislamiento 35 y el dispositivo crítico 43 44. Los medios de control 33 de nuevo cambian el estado de los medios de aislamiento 35 de tal manera que el dispositivo de almacenamiento de datos interno 34 está conectado al dispositivo crítico 43 44. A continuación, el dispositivo de almacenamiento de datos interno 34 ya no está conectado más al adaptador 30, sino únicamente al dispositivo crítico 43 44. El medio de almacenamiento de datos interno 34 que comprende los ficheros válidos 615b está ahora disponible únicamente en el dispositivo crítico 43 44, que puede detectar o leer el medio de almacenamiento de datos interno 34, y por lo tanto los ficheros 615b almacenados en estos medios de almacenamiento de datos internos 34 pueden usarse (leerse, ejecutarse). Esto se representa por la referencia 615c en la Figura 10. El adaptador 30 a continuación vuelve a su posición o estado en espera (etapa inicial 400). El dispositivo de almacenamiento de datos externo 61 puede ahora opcionalmente recuperarse/desconectarse del adaptador 30. Cuando un nuevo dispositivo de almacenamiento de datos externo se enchufa en el puerto o enchufe 31 en el adaptador 30, el proceso empieza de nuevo.

El proceso finaliza cuando el adaptador 30 está en estado “en espera” de nuevo (“Fin” o etapa 407) y los ficheros se han copiado/ejecutado del dispositivo de almacenamiento de datos interno 34 al dispositivo crítico 43 44 (fichero 615c en la Figura 10).

En conclusión, el método propuesto, el sistema permite evitar ataques originados en sistemas de almacenamiento de datos.

Por otra parte, la invención evidentemente no está limitada a la realización o realizaciones específicas descritas en el presente documento, sino que también abarca cualesquiera variaciones que puedan considerare por cualquier experto en la materia (por ejemplo, en lo que respecta a la elección de materiales, dimensiones, componentes, configuración, etc.), dentro del alcance general de la invención como se define en las reivindicaciones.

REIVINDICACIONES

1. Un sistema de seguridad (1) para evitar ataques cibernéticos en un sistema que comprende una pluralidad de dispositivos informáticos (41, 42, 43, 44), comprendiendo el sistema de seguridad (1):

- al menos un dispositivo de control (11, 12, 13) que comprende:

  - medios (112) para autenticar un usuario que intenta acceder físicamente a una zona que comprende al menos un dispositivo informático de dicha pluralidad de dispositivos informáticos (41,42, 43, 44);
  - medios para autenticar un dispositivo de almacenamiento de datos que dicho usuario pretende insertar en al menos uno de estos dispositivos informáticos (41, 42, 43, 44) y para verificar, limpiar y encriptar el contenido de dicho dispositivo de almacenamiento de datos:
  - medios para, si el dispositivo de almacenamiento de datos llevado por dicho usuario es un dispositivo de almacenamiento de datos privado, proporcionar (113) un dispositivo de almacenamiento de datos corporativo, en donde dicho dispositivo de almacenamiento de datos corporativo proporcionado comprende una copia del contenido originalmente almacenado verificado, limpiado y encriptado en dicho dispositivo de almacenamiento de datos privado;

- un agente de software (20) instalado en al menos uno de dicha pluralidad de dispositivos informáticos (41, 42), estando configurado dicho agente de software (20): para detectar si un dispositivo de almacenamiento de datos insertado en un puerto de dicho dispositivo informático (41, 42) es uno privado o uno corporativo; para, en el caso de uno privado, denegar el acceso del dispositivo de almacenamiento de datos a ese dispositivo informático (41, 42); y para, en el caso de uno corporativo, comprobar si su contenido ha sido verificado, limpiado y encriptado por un dispositivo de control (11, 12, 13) y, en el caso en que lo haya sido, desencriptar el contenido de dicho dispositivo de almacenamiento de datos corporativo, permitiendo por lo tanto que dicho dispositivo informático (41, 42) lea o ejecute dicho contenido.

2. El sistema de seguridad (1) de la reivindicación 1, en el que dicho dispositivo de almacenamiento de datos es una unidad de USB, o una mini unidad de USB, o una micro unidad de USB, o un DVD, o un CD, o una tarjeta SD, o una mini tarjeta de SD o una micro tarjeta de SD, o un disco duro portátil o cualquier otro formato del sistema de almacenamiento de datos.

3. El sistema de seguridad (1) de cualquier reivindicación anterior, en el que dichos medios (112) para autenticar un usuario comprenden medios para leer una tarjeta de acceso o un identificador electrónico de dicho usuario, en donde dichos medios para leer una tarjeta o un identificador electrónico comprenden una ranura para insertar una tarjeta o un lector inalámbrico para detectar inalámbricamente la información registrada en la tarjeta o en el identificador electrónico.

4. El sistema de seguridad (1) de cualquier reivindicación anterior, que comprende adicionalmente al menos un adaptador (30) que comprende un primer puerto (31) configurado para recibir un dispositivo de almacenamiento de datos externo (61) y un segundo puerto (32) configurado para ser enchufado en un correspondiente puerto de un dispositivo informático (43, 44) de dicha pluralidad de dispositivos informáticos (41, 42, 43, 44), proporcionando dicho al menos un adaptador (30) una interfaz física entre dicho dispositivo de almacenamiento de datos externo (61) y dicho dispositivo informático (43, 44) mientras se aísla dicho dispositivo informático (43, 44) de dicho dispositivo de almacenamiento de datos externo (61).

5. El sistema de seguridad (1) de la reivindicación 4, en el que dicho adaptador (30) comprende medios para detectar si dicho dispositivo de almacenamiento de datos (61) insertado en dicho puerto (31) del adaptador (30) es uno privado o uno corporativo; para, en el caso de uno privado, denegar al dispositivo de almacenamiento de datos (61) acceso a ese dispositivo informático (43, 44); y para, en el caso de uno corporativo, comprobar si su contenido ha sido verificado, limpiado y encriptado por un dispositivo de control (11, 12, 13) y, en el caso en que lo haya sido, desencriptar el contenido de dicho dispositivo de almacenamiento de datos, permitiendo por lo tanto que dicho dispositivo informático (43, 44) lea o ejecute dicho contenido.

6. Un método para evitar ataques cibernéticos en un sistema que comprende una pluralidad de dispositivos informáticos (41, 42, 43, 44), comprendiendo el método:

- en al menos un dispositivo de control (11, 12, 13):

  - autenticar (112) un usuario que intenta acceder físicamente a una zona que comprende al menos parte de dicho sistema que comprende una pluralidad de dispositivos informáticos (41, 42, 43, 44);
  - autenticar un dispositivo de almacenamiento de datos que dicho usuario pretende insertar en al menos uno de estos dispositivos informáticos (41, 42, 43, 44) y verificar, limpiar y encriptar el contenido de dicho dispositivo de almacenamiento de datos, en donde dicho dispositivo de almacenamiento de datos es uno corporativo o uno privado;
  - si el dispositivo de almacenamiento de datos llevado por dicho usuario es un dispositivo de almacenamiento

de datos privado, proporcionar (113) un dispositivo de almacenamiento de datos corporativo, en donde dicho dispositivo de almacenamiento de datos corporativo proporcionado comprende una copia del contenido originalmente almacenado verificado, limpiado y encriptado en dicho dispositivo de almacenamiento de datos privado;

- en al menos uno (41, 42) de dicha pluralidad de dispositivos informáticos (41, 42, 43, 44):

- detectar si un dispositivo de almacenamiento de datos insertado en un puerto de dicho dispositivo informático (41, 42) es uno privado o uno corporativo;
- si es uno privado, denegar el acceso del dispositivo de almacenamiento de datos a ese dispositivo informático (41, 42); y
- si es uno corporativo, comprobar si su contenido ha sido verificado, limpiado y encriptado por un dispositivo de control (11, 12, 13) y, en el caso en que lo haya sido, desencriptar el contenido de dicho dispositivo de almacenamiento de datos, permitiendo por lo tanto que dicho dispositivo informático (41, 42) lea o ejecute dicho contenido.

7. El método de la reivindicación 6, en el que dicha etapa de autenticación de usuario (112) comprende leer una tarjeta de acceso o un identificador electrónico de dicho usuario, en donde dicha lectura de tarjeta o identificador electrónico se realiza insertando dicha tarjeta en una ranura o detectando inalámbricamente la información registrada en la tarjeta o en el identificador electrónico;
y en donde dicha etapa de autenticación del dispositivo de almacenamiento de datos comprende comparar un identificador asociado al dispositivo de almacenamiento de datos con los identificadores comprendidos en una lista de identificadores que corresponden a respectivos dispositivos de almacenamiento de datos corporativos.

8. El método de cualquiera de las reivindicaciones 6-7, que comprende adicionalmente, después de autenticar (112) dicho usuario y autenticar dicho dispositivo de almacenamiento de datos:

- copiar el contenido de dicho dispositivo de almacenamiento de datos, en uno corporativo o en uno privado, en medios de memoria comprendidos en dicho al menos un dispositivo de control (11, 12, 13);
- eliminar de dicho contenido copiado cualquier software maligno;
- verificar que dicho contenido copiado pertenece a una lista de ficheros permitidos o extensiones de fichero permitidas;
- crear un fichero en dicha memoria significa que dicho fichero comprende el contenido sin software maligno que pertenece a dicha lista de ficheros permitidos;
- copiar dicho fichero creado en dicho dispositivo de almacenamiento de datos corporativo.

9. El método de la reivindicación 8, en el que antes de copiar dicho fichero creado en dicho dispositivo de almacenamiento de datos corporativo:

- se encripta simétricamente el fichero;
- se hace un troceo para comprobar su integridad;
- se firma el fichero encriptado y troceado con una clave privada.

10. El método de cualquiera de las reivindicaciones 6-9, en el que dicha etapa de detección en al menos uno (41, 42) de dicha pluralidad de dispositivos informáticos (41, 42, 43, 44), si el dispositivo de almacenamiento de datos insertado en un puerto de dicho dispositivo informático (41, 42) es uno privado o uno corporativo, comprende: comparar un identificador de dicho dispositivo de almacenamiento de datos insertado con cada identificador de una lista de identificadores que corresponden a dispositivos de almacenamiento de datos corporativos.

11. El método de cualquiera de las reivindicaciones 6-10, en el que dicho dispositivo de almacenamiento de datos es una unidad de USB, o una mini unidad de USB, o una micro unidad de USB, o un DVD, o un CD, o una tarjeta SD, o una mini tarjeta de SD o una micro tarjeta de SD, o un disco duro portátil o cualquier otro formato de sistema de almacenamiento de datos.

12. El método de cualquiera de las reivindicaciones 6-11, que comprende adicionalmente, en al menos uno (43, 44) de dicha pluralidad de dispositivos informáticos (41, 42, 43, 44);

- enchufar en un puerto (436) de dicho al menos un dispositivo informático (43, 44) un adaptador (30) que comprende un primer puerto (31) configurado para recibir un dispositivo de almacenamiento de datos externo (61), estando enchufado dicho adaptador (30) en dicho puerto (436) del dispositivo informático (43, 44) a través de un puerto (32) del adaptador (30);
- enchufar en dicho primer puerto (31) de dicho adaptador (30) un dispositivo de almacenamiento de datos externo (61);
- proporcionar por dicho adaptador (30) una interfaz física entre dicho dispositivo de almacenamiento de datos externo (61) y dicho dispositivo informático (43, 44) mientras se aísla dicho dispositivo informático (43, 44) de dicho dispositivo de almacenamiento de datos externo (61).

13. El método de la reivindicación 12, que comprende adicionalmente en dicho adaptador (30): detectar si el dispositivo de almacenamiento de datos (61) insertado en dicho puerto (31) del adaptador (30) es uno privado o uno corporativo; si es uno privado, denegar al dispositivo de almacenamiento de datos (61) acceso a ese dispositivo informático (43, 44); y si es uno corporativo, comprobar si su contenido (615) ha sido verificado, limpiado y encriptado por un dispositivo de control (11, 12, 13) y, en el caso en que lo haya sido, desencriptar el contenido de dicho dispositivo de almacenamiento de datos (61), permitiendo por lo tanto que dicho dispositivo informático (43, 44) lea o ejecute dicho contenido (615c).

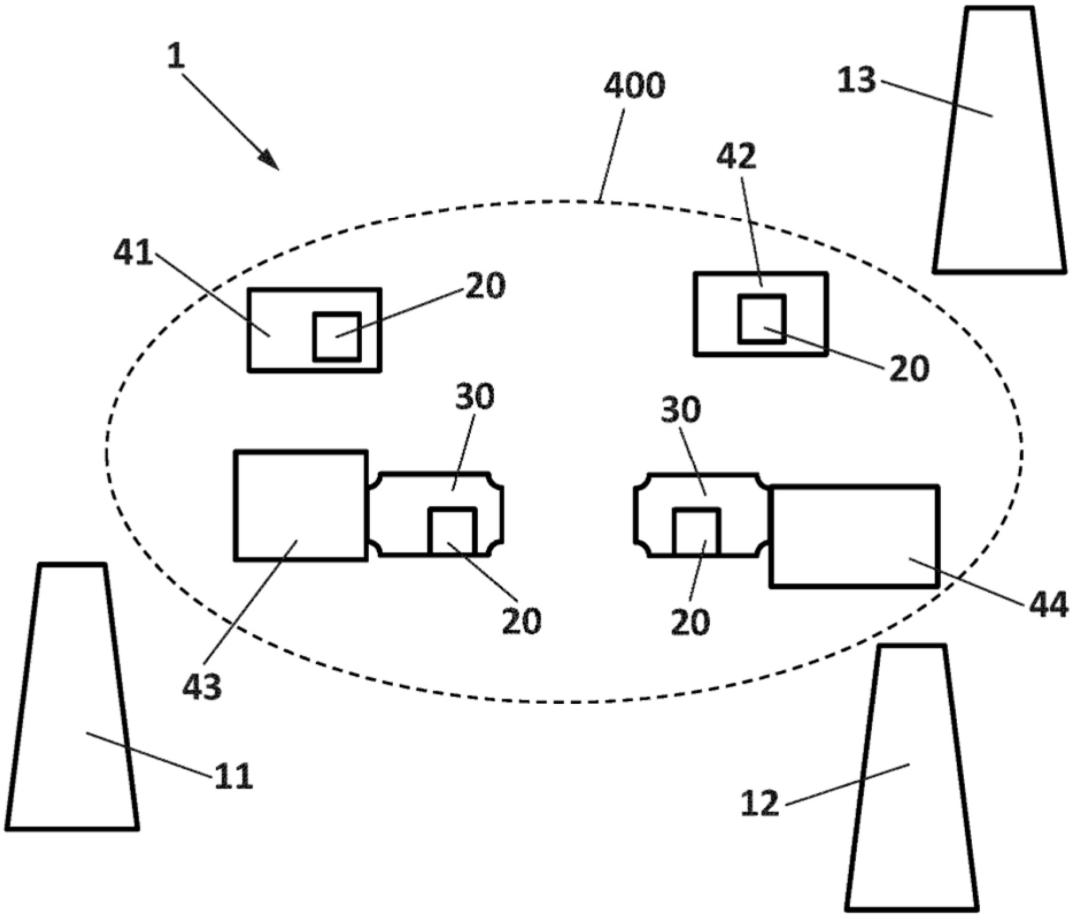

FIG. 1

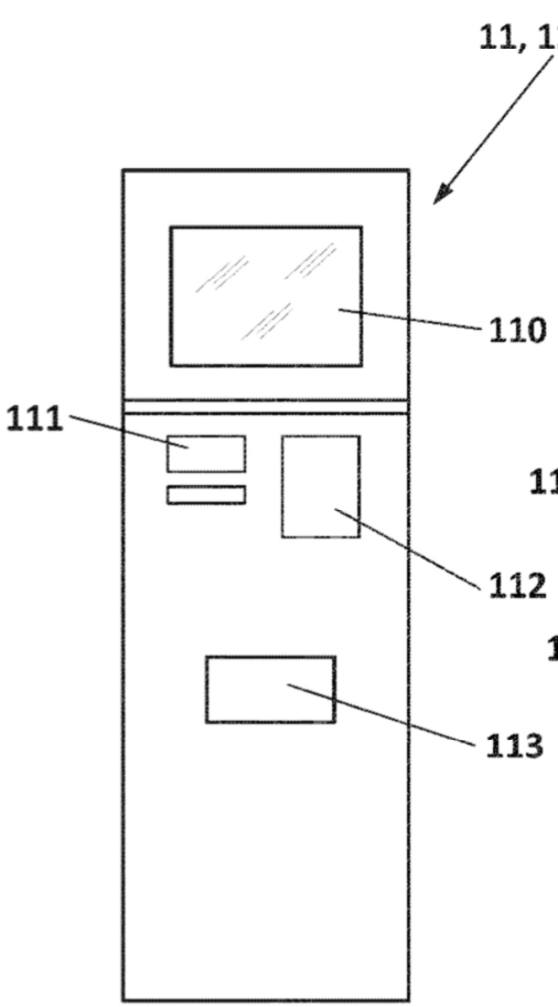

FIG. 2A

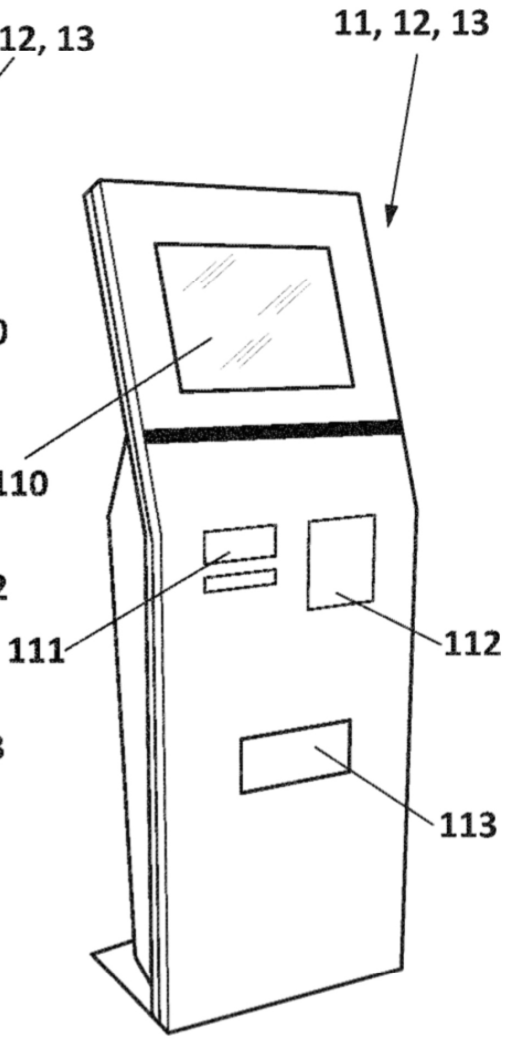

FIG. 2B

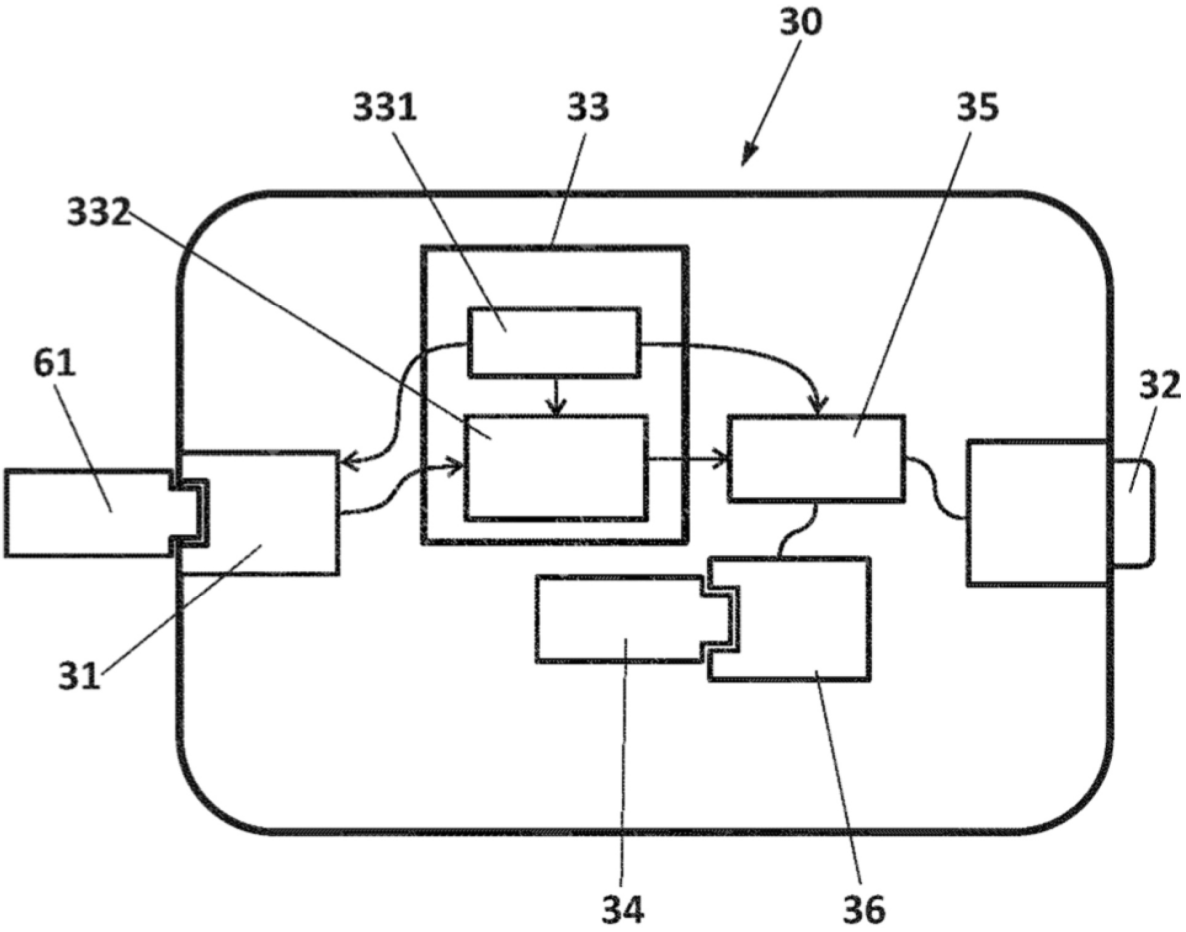

FIG. 3

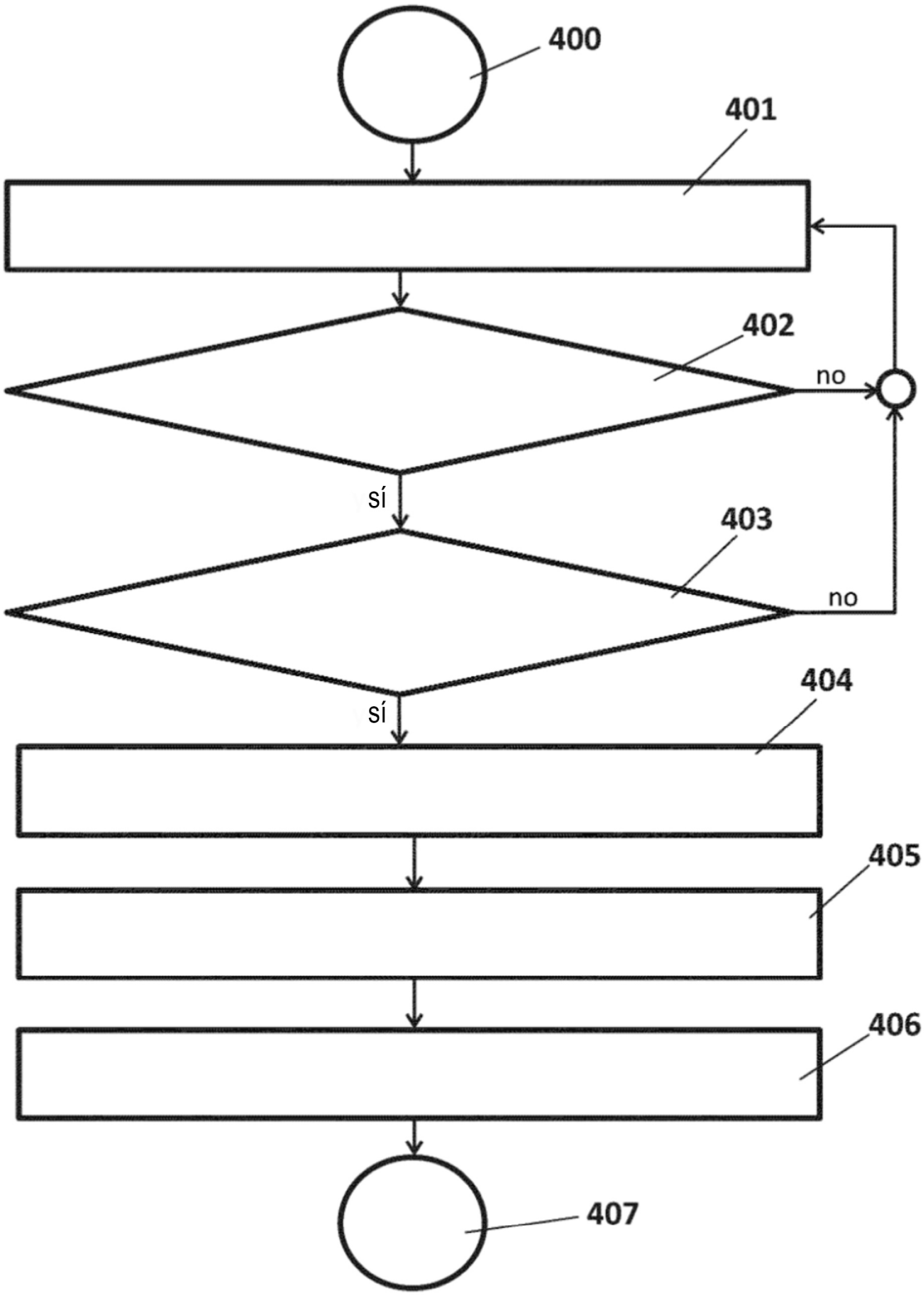

FIG. 4

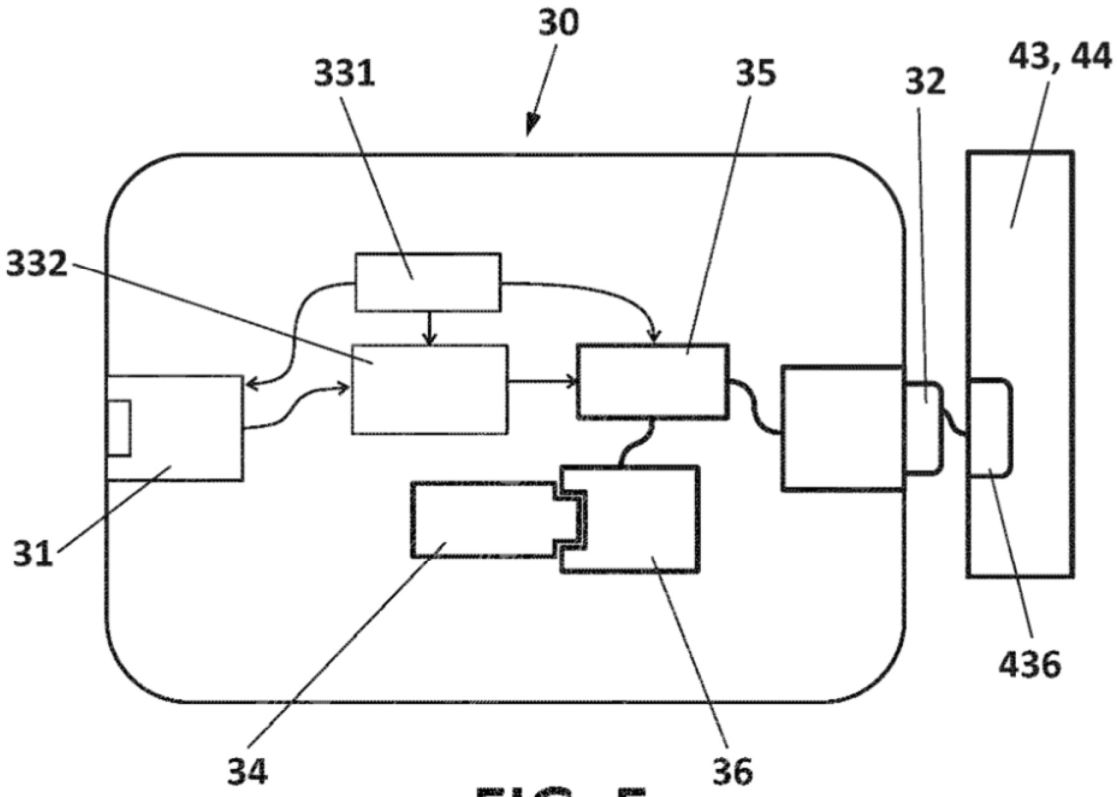
30
331
35
32
43, 44
332
31
34
36
436

FIG. 5

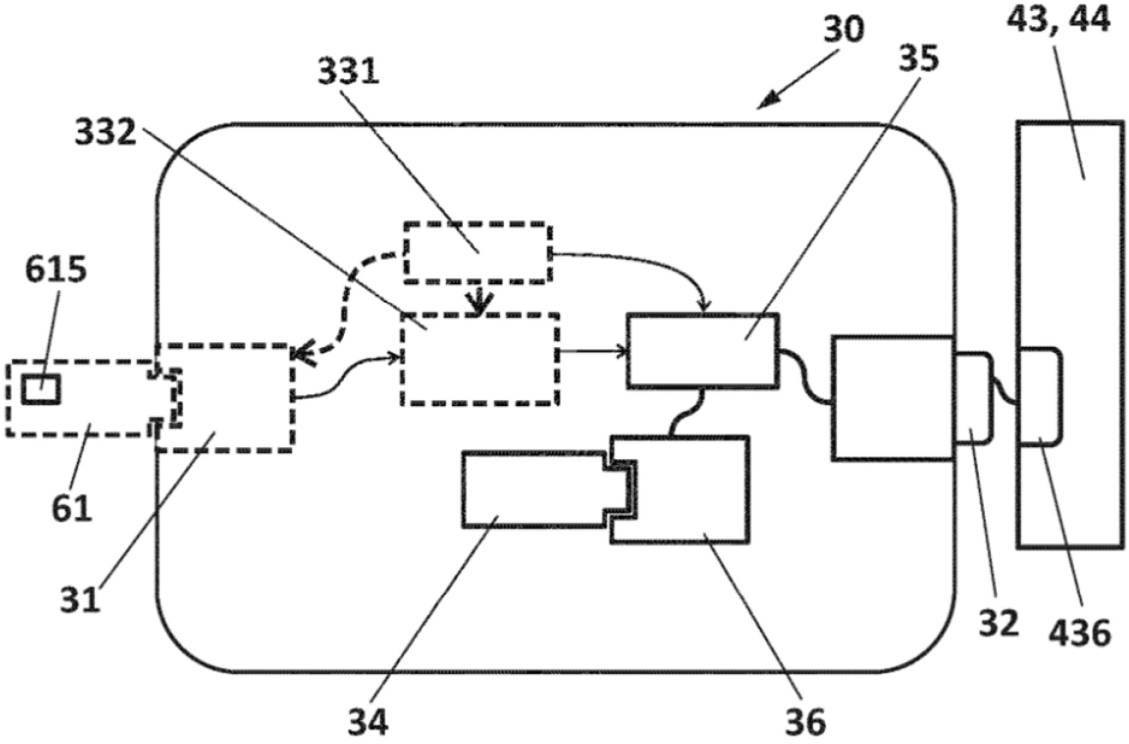
30
331
35
43, 44
332
615
61
31
34
36
32
436

FIG. 6

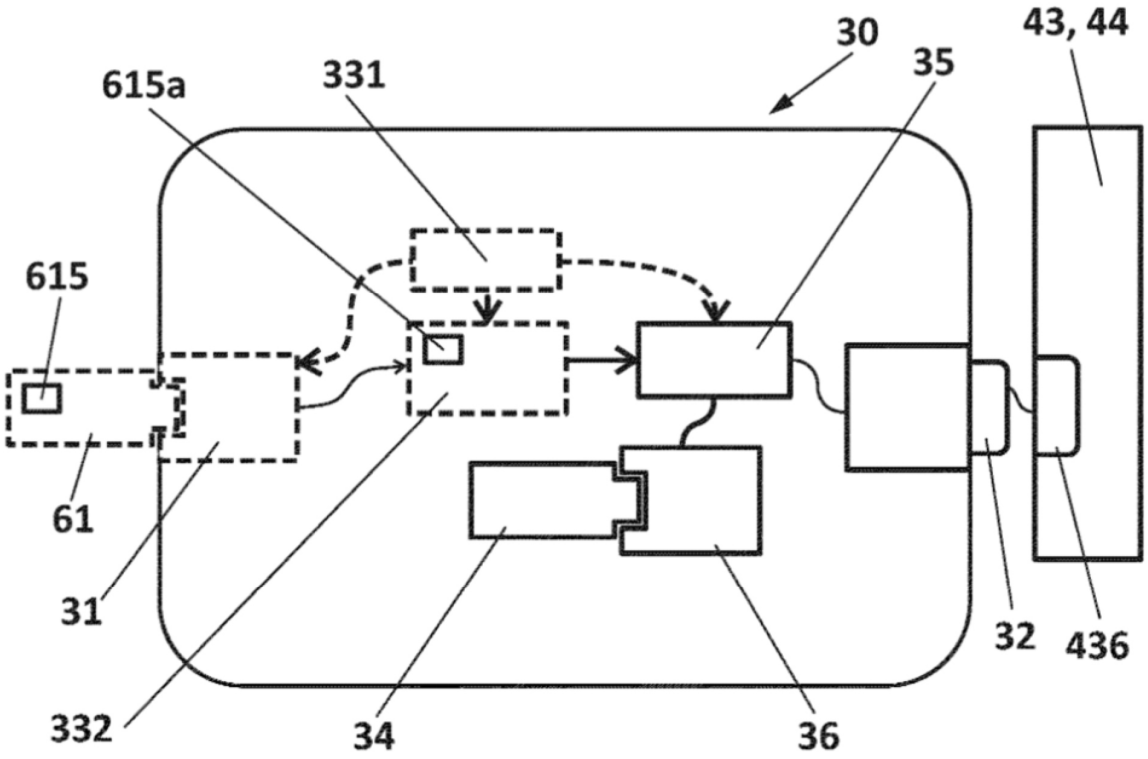
30
43, 44
615a
331
35
615
61
31
332
34
36
32
436

FIG. 7

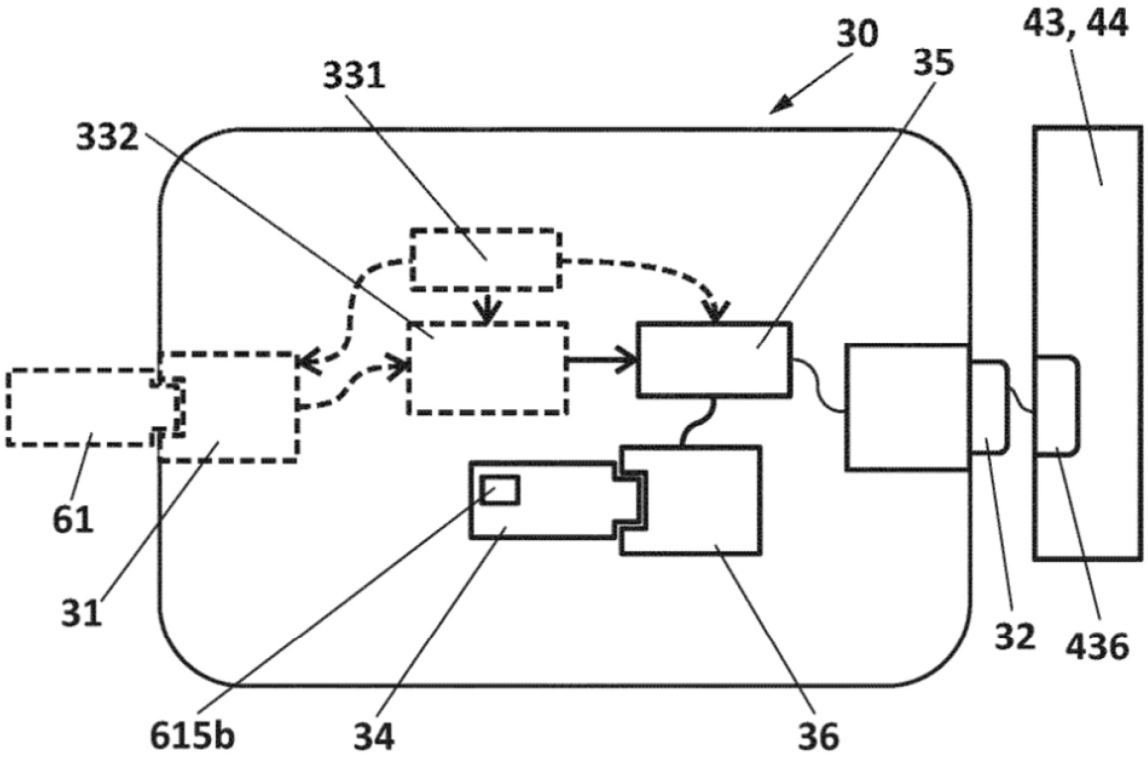
30
43, 44
331
35
332
61
31
615b
34
36
32
436

FIG. 8

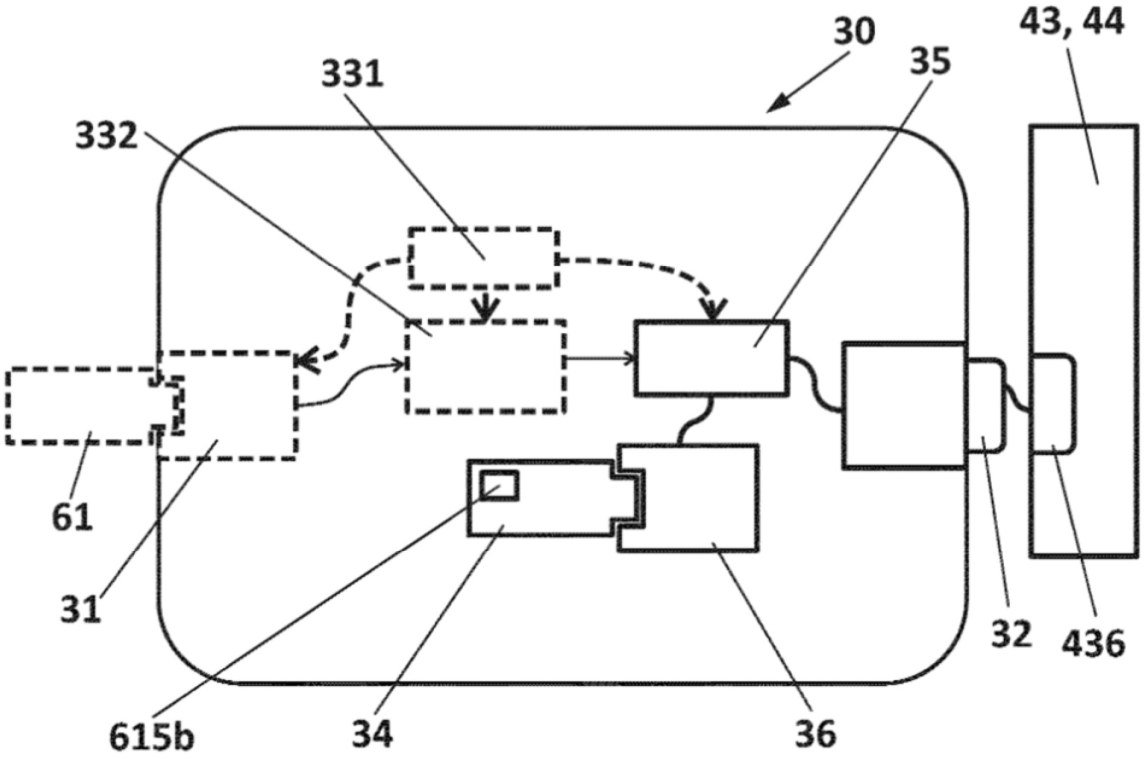
30
35
43, 44
331
332
61
31
615b
34
36
32
436

FIG. 9

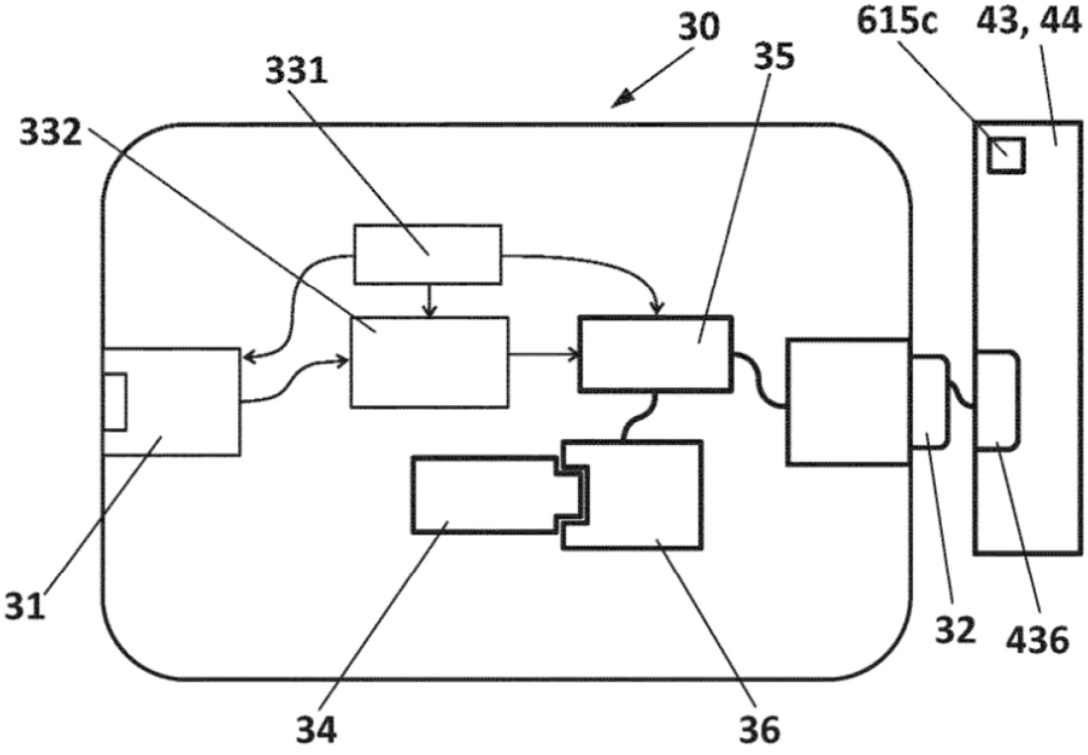
30
35
615c
43, 44
331
332
31
34
36
32
436

FIG. 10