

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 980 714**

51 Int. Cl.:

G06F 21/44 (2013.01)

H04L 9/40 (2012.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **28.06.2021** **PCT/EP2021/067632**

87 Fecha y número de publicación internacional: **06.01.2022** **WO22002823**

96 Fecha de presentación y número de la solicitud europea: **28.06.2021** **E 21737601 (1)**

97 Fecha y número de publicación de la concesión europea: **01.05.2024** **EP 4176361**

54 Título: **Procedimiento y sistema para la puesta en servicio o la gestión de un dispositivo de control fuera de línea**

30 Prioridad:

01.07.2020 DE 102020117287

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

02.10.2024

73 Titular/es:

SPHINX ELECTRONICS GMBH & CO KG (100.0%)
Tullastrasse 3
79341 Kenzingen, DE

72 Inventor/es:

CHENG, TRONG-NGHIA;
EGGERT, REINHARD y
BODECHON, PASCAL

74 Agente/Representante:

ISERN JARA, Nuria

ES 2 980 714 T3

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

DESCRIPCIÓN

Procedimiento y sistema para la puesta en servicio o la gestión de un dispositivo de control fuera de línea

5 La invención se refiere a un procedimiento y a un sistema para la puesta en servicio y la gestión de un dispositivo de control fuera de línea, en particular un dispositivo de control de acceso fuera de línea, mediante autenticación multifactor/ID.

Normalmente, los terminales producidos por el fabricante se entregan desprotegidos y accesibles a terceros (clientes).

10 Solo a través de una autenticación multifactor se atribuyen "permisos" al terminal para permitir una puesta en servicio (inicial) protegida/segura. A partir de este momento, el terminal queda protegido contra "accesos" no autorizados.

El documento CN 109 271 757 A divulga un procedimiento para la puesta en servicio y la gestión de software fuera de línea con las siguientes etapas de procedimiento para la puesta en servicio inicial del software:

- 15
- implementar un algoritmo de autenticación en un terminal, en particular por parte del fabricante del terminal,
 - entregar el terminal en condiciones de funcionamiento y un primer medio de almacenamiento, en particular móvil, en el que está almacenado un primer código de seguridad, a un cliente, en particular por parte del proveedor del software,
 - 20 - entregar un segundo código de seguridad, generado con ayuda del primer código de seguridad, en particular por el fabricante del terminal, a un segundo medio de almacenamiento, en particular a un terminal móvil, del cliente, en particular por parte del proveedor del software,
 - colocar el primer y el segundo medio de almacenamiento en la ubicación del terminal por parte de un usuario y leer el primer y el segundo código de seguridad por parte del terminal y verificar fuera de línea. mediante el terminal,
 - 25 - si el primer y el segundo código de seguridad leídos son mutuamente válidos,
 - tras una verificación positiva, activar el software por parte del terminal para la gestión del software por parte del usuario, y
 - poner fin al modo de puesta en servicio inicial.

30 El documento CN 105 915 343 B se refiere a la activación fuera de línea de un usuario registrado con las siguientes etapas de procedimiento:

- una nube captura un primer código de activación enviado por el usuario y analiza el primer código de activación para determinar si el usuario es un usuario registrado,
- 35 - en caso afirmativo, se genera un primer código de verificación correspondiente al primer código de activación de acuerdo con una regla de generación de código de verificación y se envía al usuario,
- un cliente recibe el primer código de verificación cargado por el usuario y verifica el primer código de verificación de acuerdo con una regla de verificación y, si la verificación es satisfactoria, activa al usuario registrado.

40 La invención se basa en el objetivo de garantizar que, en un dispositivo de control fuera de línea, es decir, que no está conectado a Internet, solo se autorice una persona autorizada para ello o a un dispositivo autorizado.

Este objetivo se logra de acuerdo con la invención mediante un procedimiento para la puesta en servicio y la gestión de un dispositivo de control fuera de línea, en particular un dispositivo de control de acceso fuera de línea, mediante autenticación multifactor/ID, en donde el dispositivo de control presenta una unidad de control de gestión (por ejemplo, Connect Modular Core) y un terminal que activa la unidad de control de gestión, con las siguientes etapas de procedimiento para la puesta en servicio inicial del dispositivo de control:

- 45
- implementar un algoritmo de autenticación multifactor/ID en el terminal, en particular por parte del fabricante del terminal,
 - entregar el terminal en estado de fábrica y un primer medio de almacenamiento, en particular móvil, (p. ej. un transpondedor AKC), en el que están almacenados a prueba de falsificaciones y de forma única para todo el mundo un ID de medio de almacenamiento (p. ej. un transpondedor UID (Unique Identifier)) y un primer código de seguridad (primer factor, por ejemplo, Secure Token), a un cliente, en particular por parte del proveedor del dispositivo de control,
 - 50 - entregar un segundo código de seguridad (segundo factor, por ejemplo, Secure Signature, que está guardado (empaquetado) en un archivo de licencia), generado con ayuda del primer código de seguridad, en particular por el fabricante del terminal, a un segundo medio de almacenamiento, en particular a un terminal móvil (por ejemplo, un teléfono inteligente), del cliente, en particular por parte del proveedor del dispositivo de control,
 - 60 - colocar el primer y el segundo medio de almacenamiento (por ejemplo, un transpondedor AKC y un teléfono inteligente) en la ubicación del terminal por parte de un usuario y leer el ID de medio de almacenamiento y el primer y el segundo código de seguridad por parte del terminal y verificar fuera de línea, mediante el algoritmo de autenticación multifactor del terminal, si los códigos de seguridad primero y segundo leídos son mutuamente válidos,
 - 65 - tras una verificación de autenticación multifactor positiva, almacenar el ID de medio de almacenamiento como ID de autorización y el primer código de seguridad en el terminal y, dado el caso, activar a continuación la unidad de

- control de gestión por parte del terminal para la gestión de la unidad de control de gestión por parte del usuario, y
- poner fin al modo de puesta en servicio inicial y, una vez completada la puesta en servicio inicial del dispositivo de control, con las siguientes etapas de procedimiento para gestionar la unidad de control de gestión:
- colocar dos medios de almacenamiento (por ejemplo, un transpondedor AKC y un teléfono inteligente) en la ubicación del terminal por parte de un usuario y leer un ID de medio de almacenamiento y un código de seguridad de uno de los medios de almacenamiento (por ejemplo, el transpondedor AKC) y un código de seguridad del otro medio de almacenamiento (por ejemplo, el teléfono inteligente) por parte del terminal y verificar fuera de línea, mediante el algoritmo de autenticación multifactor/ID del terminal, si el ID de medio de almacenamiento leído y el código de seguridad leído de uno de los medios de almacenamiento coinciden con el ID de autorización almacenado en el terminal y el primer código de seguridad almacenado en el terminal y si los dos códigos de seguridad leídos son mutuamente válidos,
- tras una verificación de autenticación multifactor/ID positiva, activar la unidad de control de gestión por parte del terminal para la gestión de la unidad de control de gestión por parte del usuario, y
- poner fin al modo de gestión.

En el modo de gestión, la verificación de autenticación multifactor se lleva a cabo preferentemente solo tras una verificación de autenticación de ID positiva.

El procedimiento de acuerdo con la invención asegura una comunicación con la unidad de control (por ejemplo, Connect Modular Core) realizando una autenticación multifactor (MFA) antes de cada inicio de comunicación. Para ello, antes de la comunicación propiamente dicha del cliente (modo de puesta en marcha inicial o de gestión) con la unidad de control se realiza una verificación mediante al menos dos características de autorización diferentes mediante códigos de seguridad y medios de almacenamiento. Tanto la validez como el número de los primeros medios de almacenamiento (p. ej. transpondedor AKC (Autorisation Key Card)) pueden configurarse según se desee por el fabricante del terminal. La ventaja del procedimiento radica en que todos los componentes se pueden verificar "fuera de línea", es decir, a través de una conexión directa sin pasar por Internet u otra red. El terminal por sí solo valida los códigos de seguridad, que son generados exclusivamente por el fabricante del terminal. El comprador de los terminales, es decir, el cliente, no conoce los códigos de seguridad y, por tanto, no puede transmitirlos a personas no autorizadas. Esto garantiza un alto nivel de seguridad.

Preferiblemente, el primer código de seguridad (por ejemplo, Secure Token) se almacena en un transpondedor (por ejemplo, transpondedor RFID) suministrado al cliente, por ejemplo en forma de un código binario con al menos 16 bytes. Con un código binario con 16 bytes hay 2^{16} formas de generar un código binario de 16 bytes, por lo que dicho código binario ofrece un alto nivel de seguridad.

La transmisión de un ID de medio de almacenamiento y/o de un código de seguridad de un medio de almacenamiento colocado en la ubicación del terminal (por ejemplo, un transpondedor AKC, un teléfono inteligente) al terminal se realiza preferentemente de forma inalámbrica o por cable, en particular mediante RFID o Bluetooth, o sea fuera de línea, es decir, a través de una conexión directa y sin pasar por Internet u otra red.

Preferiblemente, el segundo código de seguridad (por ejemplo, Secure Signature) se entrega como una firma digital del primer código de seguridad a un terminal móvil del cliente, en particular un teléfono inteligente. Para ello, el segundo código de seguridad puede cifrarse ventajosamente con una clave privada del fabricante del terminal y la validez del segundo código de seguridad cifrado puede verificarse mediante el algoritmo de autenticación del terminal con una clave pública del fabricante del terminal. Por ejemplo, se puede usar un Digital Signature Algorithm (DSA) o un Elliptic Curve Digital Signature Algorithm (ECDSA) para el cifrado y se puede usar un algoritmo definido en el Federal Information Processing Standard (FIPS) o el Digital Signature Standard (DSS) para generar la firma digital. Las claves públicas y privadas se generan en el marco del DSA o el ECDSA.

Para generar el segundo código de seguridad, por ejemplo, se puede determinar un valor *hash* del primer código de seguridad con ayuda de una función *hash* criptográfica que se aplica al primer código de seguridad y luego se puede aplicar la clave privada del fabricante del terminal a este valor *hash* del primer código de seguridad para generar el segundo código de seguridad en forma de una firma digital del primer código de seguridad, por ejemplo en forma de un archivo de licencia digital. Las funciones *hash* o funciones de valores de dispersión se utilizan para correlacionar valores de entrada en forma de cadenas de caracteres de cualquier longitud con cadenas de caracteres de longitud fija, los valores *hash*, en particular números naturales. Las funciones *hash* criptográficas están en particular prácticamente libres de colisiones, lo que significa, en particular, que existe una probabilidad extremadamente baja de que diferentes valores de entrada se correlacionan con diferentes valores *hash* idénticos. En particular, se utiliza una función *hash* de la familia Secure Hash Algorithm-2 (SHA-2) o de la familia SHA-3.

El segundo código de seguridad (por ejemplo, Secure Signature) se puede transmitir de forma inalámbrica, en particular mediante Bluetooth, desde el segundo medio de almacenamiento (por ejemplo, un teléfono inteligente) al terminal, en particular fuera de línea, es decir, a través de una conexión directa sin pasar por Internet u otra red.

La invención también se refiere a un sistema adecuado para llevar a cabo el procedimiento de acuerdo con la invención para la puesta en servicio y la gestión de un dispositivo de control fuera de línea, en particular un dispositivo de control

de acceso fuera de línea, mediante autenticación multifactor/ID, que comprende:

- un dispositivo de control que presenta una unidad de control de gestión (por ejemplo, Connect Modular Core) y un terminal que activa la unidad de control de gestión con al menos una interfaz de datos, en donde en el terminal está implementado un algoritmo de autenticación multifactor/ID y se pueden almacenar al menos un ID de autorización y un código de seguridad,
 - un primer medio de almacenamiento móvil (por ejemplo, un transpondedor AKC), en el que están almacenados a prueba de falsificaciones un ID de medio de almacenamiento (por ejemplo, un transpondedor UID (Unique Identifier)) y un primer código de seguridad (primer factor, por ejemplo, Secure Token),
 - un segundo medio de almacenamiento móvil, en particular un dispositivo móvil (por ejemplo, un teléfono inteligente), en el que está almacenado un segundo código de seguridad (segundo factor, por ejemplo, Secure Signature, que está guardado (empaquetado) en un archivo de licencia) generado con ayuda del primer código de seguridad, en donde el algoritmo de autenticación multifactor/ID para la puesta en servicio inicial del dispositivo de control está programado para, en el caso de dos medios de almacenamiento colocados en la ubicación del terminal por un usuario (por ejemplo, un transpondedor AKC y un teléfono inteligente), leer un ID de medio de almacenamiento y un código de seguridad de uno de los medios de almacenamiento y un código de seguridad del otro medio de almacenamiento mediante la al menos una interfaz de datos y verificar fuera de línea si el primer y el segundo código de seguridad leídos son mutuamente válidos y, de ser así, almacenar el ID de medio de almacenamiento como ID de autorización y el primer código de seguridad en el terminal y poner fin al modo de puesta en servicio inicial, y en donde el algoritmo de autenticación multifactor/ID para la gestión de la unidad de control de gestión está programado para, en el caso de dos medios de almacenamiento colocados en la ubicación del terminal por un usuario (por ejemplo, un transpondedor AKC y un teléfono inteligente) leer un ID de medio de almacenamiento y un código de seguridad de uno de los medios de almacenamiento y un código de seguridad del otro medio de almacenamiento mediante la al menos una interfaz de datos y verificar fuera de línea si el ID de medio de almacenamiento leído y el código de seguridad leído de uno de los medios de almacenamiento coinciden con el ID de autorización almacenado en el terminal y con el primer código de seguridad almacenado en el terminal y si los dos códigos de seguridad leídos son mutuamente válidos y, de ser así, activar la unidad de control de gestión para la gestión por parte del usuario y poner fin al modo de gestión.
- Preferiblemente, el algoritmo de autenticación multifactor/ID está programado para llevar a cabo la verificación de autenticación multifactor en el modo de gestión solo tras una verificación de autenticación de ID positiva y/o para activar la unidad de control de gestión para la gestión de la unidad de control de gestión por parte del usuario en el modo de puesta en marcha inicial tras almacenar el ID de autorización.
- Mediante dos códigos de seguridad diferentes, desconocidos para el usuario del dispositivo de control fuera de línea, en dos medios de almacenamiento diferentes y mediante su verificación separada mediante el algoritmo de autenticación multifactor/ID, el sistema ofrece un alto nivel de seguridad, incluso si uno de los dos códigos de seguridad pasa a ser conocido por terceros.
- El primer medio de almacenamiento puede ser preferentemente un transpondedor, en particular un transpondedor RFID, y el terminal puede presentar una interfaz de datos, en particular una interfaz RFID, para la lectura inalámbrica de los datos almacenados en el transpondedor, como por ejemplo el primer código de seguridad. Los transpondedores RFID permiten el intercambio directo de datos a distancias cortas, independientemente de otros canales de comunicación como Internet. Los transpondedores RFID también se caracterizan por su diseño compacto. En particular se utilizan transpondedores RFID "ISO/IEC 14443 A 1-4".
- El segundo medio de almacenamiento puede ser preferentemente un terminal móvil del cliente, en particular un teléfono inteligente, y el terminal puede presentar una interfaz de datos, en particular una interfaz Bluetooth, para la lectura inalámbrica de los datos almacenados en el terminal móvil, como por ejemplo el segundo código de seguridad. La interfaz Bluetooth permite el intercambio directo de datos a distancias cortas, independientemente de otros canales de comunicación como Internet.
- Preferiblemente, el primer medio de almacenamiento (AKC) tiene protección contra copia/clonación, protección contra escritura, protección contra lectura y protección contra manipulación y/o el segundo medio de almacenamiento (teléfono inteligente) tiene protección contra manipulación. Por lo tanto, los datos contenidos en los medios de almacenamiento no pueden ser modificados ni copiados por personas no autorizadas.
- Es especialmente preferible que una aplicación AKC (Autorisation Key Card) del proveedor, activada mediante el segundo código de seguridad (por ejemplo, Secure Signature) para la gestión de la unidad de control de gestión, esté instalada en un terminal móvil (por ejemplo, un teléfono inteligente) del cliente.

Otras ventajas de la invención se desprenden de la descripción, las reivindicaciones y el dibujo. Asimismo, las características mencionadas anteriormente y las que se detallan a continuación se pueden utilizar cada una individualmente o en grupos en cualquier combinación. Las formas de realización mostradas y descritas no han de entenderse como una lista exhaustiva, sino que, por el contrario, tienen un carácter de ejemplo para ilustrar la invención.

Muestra:

5 la Fig. 1 una representación esquemática del sistema de acuerdo con la invención para la puesta en servicio o la gestión de un dispositivo de control fuera de línea.

El sistema 1 mostrado en la Fig. 1 se utiliza para la puesta en servicio y la gestión de un dispositivo de control fuera de línea 2, tal como un dispositivo de control de acceso fuera de línea, mediante autenticación multifactor/ID.

10 El sistema comprende

- una unidad de control de puesta en servicio/gestión 3,
- un terminal 4 que activa la unidad de control 3, en el que se puede almacenar un primer código de seguridad (primer factor, por ejemplo, Secure Token) 5 conocido exclusivamente por el fabricante del terminal y está
- 15 implementado un algoritmo de autenticación multifactor/ID 6,
- un primer medio de almacenamiento 7 móvil, en lo sucesivo únicamente a modo de ejemplo en forma de un transpondedor, tal como un transpondedor RFID, en el que están almacenados a prueba de falsificaciones y de forma única para todo el mundo un ID de medio de almacenamiento (UID) del primer medio de almacenamiento 7 y el primer código de seguridad 5, y
- 20 - un segundo medio de almacenamiento 8 móvil, en lo sucesivo únicamente a modo de ejemplo en forma de un terminal móvil (por ejemplo, un teléfono inteligente), en el que está almacenado un segundo código de seguridad 22 (segundo factor, por ejemplo, Secure Signature) generado con ayuda del primer código de seguridad 5 por el fabricante del terminal.

25 El terminal 4 presenta tanto una interfaz de datos (por ejemplo, un lector RFID) 10 para leer de forma inalámbrica los datos almacenados en el transpondedor 7 (ID de medio de almacenamiento y primer código de seguridad 5) como una interfaz de datos (por ejemplo, interfaz Bluetooth) 11 para leer de forma inalámbrica el segundo código de seguridad 22 almacenado en el terminal móvil 8.

30 Un generador de aleatoriedad 12 del sistema 1 crea un primer código de seguridad 5 aleatorio, que se almacena en el transpondedor 7 en una unidad de producción de transpondedor 13. El transpondedor 7 tiene una protección contra escritura/lectura 14, que está protegida con una protección contra falsificaciones, contra copia/clonación y contra manipulación 15 que solo conoce el fabricante del terminal. Esta protección 15 contra copia/clonación y contra manipulación puede ser, por ejemplo, una codificación individual que depende del ID del transpondedor (UID).

35 Un valor *hash* 17 del primer código de seguridad 5 se determina usando una función *hash* criptográfica o un algoritmo de valor *hash* 16. En un generador (por ejemplo, generador ECDSA) 18 para criptografía asimétrica, se generan una clave pública ("public key") 19 y una clave privada ("private key") 20 del fabricante del terminal. La clave pública 19 está almacenada en el terminal 4. En una unidad de cálculo 21 se crea a partir del valor *hash* 17, mediante la clave

40 privada 20, un registro de datos, en lo sucesivo denominado firma de seguridad digital (Secure Signature) 22, que – por ejemplo, en forma de un archivo de licencia 9 que incluye opciones de licencia 100– forma el segundo código de seguridad 22. El segundo código de seguridad 22 está protegido con una protección contra manipulación 23 conocida solo por el fabricante del terminal.

45 La puesta en servicio inicial del dispositivo de control fuera de línea 2 mediante autenticación multifactor/ID se describe a continuación, usando meramente a modo de ejemplo un transpondedor 7 como primer medio de almacenamiento y un terminal móvil 8 como segundo medio de almacenamiento, y presenta las siguientes etapas de procedimiento:

- 50 - implementar el algoritmo de autenticación multifactor/ID 6 en el terminal 4 en particular por parte del fabricante del terminal,
- entregar el terminal 4 en estado de fábrica y el transpondedor 7, en el que están almacenados a prueba de falsificaciones y de forma única para todo el mundo el UID del transpondedor y el primer código de seguridad 5 (primer factor, por ejemplo, Secure Token), a un cliente, en particular por parte del proveedor del dispositivo de control 2,
- 55 - entregar el segundo código de seguridad 22 (segundo factor, por ejemplo, Secure Signature) generado con ayuda del primer código de seguridad 5 en particular por el fabricante del terminal, al terminal móvil 8 (por ejemplo, un teléfono inteligente) del cliente, en particular por parte del proveedor del dispositivo de control 2,
- colocar el transpondedor 7 y el terminal móvil 8 en la ubicación del terminal 4 por parte de un usuario y leer el UID del transpondedor y el primer y el segundo código de seguridad 5, 22 por parte del terminal 4 y verificar fuera de
- 60 línea, mediante el algoritmo de autenticación multifactor 6 del terminal 4, si los códigos de seguridad primero y segundo 5, 22 leídos son mutuamente válidos,
- tras una verificación de autenticación multifactor positiva, almacenar el UID del transpondedor como ID de autorización y el primer código de seguridad 5 en el terminal 4 y, dado el caso, activar a continuación la unidad de control de gestión 3 mediante una activación 24 del terminal 4 para la gestión de la unidad de control de gestión 3
- 65 por parte del usuario, y
- poner fin al modo de puesta en servicio inicial.

Una vez completada la puesta en servicio inicial del dispositivo de control 2, se llevan a cabo las siguientes etapas de procedimiento para gestionar la unidad de control de gestión 3:

- 5 - colocar dos medios de almacenamiento (por ejemplo, un transpondedor 7 y un terminal móvil 8) en la ubicación del terminal 4 por parte de un usuario y leer el UID del transpondedor y un código de seguridad del transpondedor 7 y un código de seguridad del terminal móvil 8 por parte del terminal 4 y comprobar fuera de línea mediante el algoritmo de autenticación multifactor/ID 6 del terminal 4, si el UID del transpondedor leído y el código de seguridad leído del transpondedor 7 coinciden con el ID de autorización almacenado en el terminal 4 y con el primer código de seguridad 5 almacenado en el terminal 4 y si los dos códigos de seguridad leídos son mutuamente válidos,
- 10 - tras una verificación de autenticación multifactor/ID positiva, activar la unidad de control de gestión 3 por parte del terminal 4 para la gestión de la unidad de control de gestión 3 por parte del usuario, y
- poner fin al modo de gestión.
- 15 El dispositivo de control 2 gestiona la autorización 25, por ejemplo de un mecanismo de bloqueo 26, y puede abrir y cerrar el mecanismo de bloqueo 26. Para accionar el mecanismo de bloqueo 26, un usuario introduce un código de acceso (por ejemplo, código PIN) 27, que se le ha comunicado, en un dispositivo de lectura (por ejemplo, lector de código PIN) 28. La autorización de acceso 25 verifica la autorización del código de acceso 27 introducido y solo acciona el mecanismo de bloqueo 26 si la verificación de autorización fue satisfactoria.

REIVINDICACIONES

1. Procedimiento para la puesta en servicio y la gestión de un dispositivo de control fuera de línea (2), en particular un dispositivo de control de acceso fuera de línea, mediante autenticación multifactor/ID, en donde el dispositivo de control (2) presenta una unidad de control de gestión (3) y un terminal (4) que activa la unidad de control de gestión (3), con las siguientes etapas de procedimiento para la puesta en servicio inicial del dispositivo de control (2):
 - implementar un algoritmo de autenticación multifactor/ID (6) en el terminal (4), en particular por parte del fabricante del terminal,
 - entregar el terminal (4) en condiciones de funcionamiento y un primer medio de almacenamiento (7), en particular móvil, en el que están almacenados a prueba de falsificaciones y de forma única para todo el mundo un ID de medio de almacenamiento y un primer código de seguridad (5), a un cliente, en particular por parte del proveedor del dispositivo de control (2),
 - entregar un segundo código de seguridad (22), generado con ayuda del primer código de seguridad (5), en particular por el fabricante del terminal, a un segundo medio de almacenamiento (8), en particular a un terminal móvil, del cliente, en particular por parte del proveedor del dispositivo de control (2),
 - colocar el primer y el segundo medio de almacenamiento (7, 8) en la ubicación del terminal (4) por parte de un usuario y leer el ID de medio de almacenamiento y el primer y el segundo código de seguridad (5, 22) por parte del terminal (4) y verificar fuera de línea, mediante el algoritmo de autenticación multifactor (6) del terminal (4), si los códigos de seguridad primero y segundo (5, 22) leídos son mutuamente válidos,
 - tras una verificación de autenticación multifactor positiva, almacenar el ID de medio de almacenamiento como ID de autorización y el primer código de seguridad (5) en el terminal (4) y, dado el caso, activar a continuación la unidad de control de gestión (3) por parte del terminal (4) para la gestión de la unidad de control de gestión (3) por parte del usuario, y
 - poner fin al modo de puesta en servicio inicial y, una vez completada la puesta en servicio inicial del dispositivo de control (2), con las siguientes etapas de procedimiento para gestionar la unidad de control de gestión (3):
 - colocar dos medios de almacenamiento en la ubicación del terminal (4) por parte de un usuario y leer un ID de medio de almacenamiento y un código de seguridad de uno de los medios de almacenamiento y un código de seguridad del otro medio de almacenamiento por parte del terminal (4) y verificar fuera de línea, mediante el algoritmo de autenticación multifactor/ID (6) del terminal (4), si el ID de medio de almacenamiento leído y el código de seguridad leído de uno de los medios de almacenamiento coinciden con el ID de autorización almacenado en el terminal (4) y con el primer código de seguridad (5) almacenado en el terminal (4) y si los dos códigos de seguridad leídos son mutuamente válidos,
 - tras una verificación de autenticación multifactor/ID positiva, activar la unidad de control de gestión (3) por parte del terminal (4) para la gestión de la unidad de control de gestión (3) por parte del usuario, y
 - poner fin al modo de gestión.
2. Procedimiento según la reivindicación 1, caracterizado por que, en el modo de gestión, la verificación de autenticación multifactor solo se lleva a cabo tras una verificación de autenticación de ID positiva.
3. Procedimiento según la reivindicación 1 o 2, caracterizado por que la transmisión de un ID de medio de almacenamiento y/o de un código de seguridad de un medio de almacenamiento colocado en la ubicación del terminal (4) al terminal (4) se realiza fuera de línea de forma inalámbrica o por cable, en particular mediante RFID o Bluetooth.
4. Procedimiento según una de las reivindicaciones anteriores, caracterizado por que el primer medio de almacenamiento (7) es un transpondedor que se entrega al cliente, en particular junto con el terminal (4).
5. Procedimiento según una de las reivindicaciones anteriores, caracterizado por que el primer código de seguridad (5) es un código binario, en particular con al menos 16 bytes.
6. Procedimiento según una de las reivindicaciones anteriores, caracterizado por que el segundo código de seguridad (22) se entrega como firma digital del primer código de seguridad (5) al segundo medio de almacenamiento (8), en particular a un terminal móvil, y se almacena allí.
7. Procedimiento según una de las reivindicaciones anteriores, caracterizado por que el segundo código de seguridad (22) se cifra mediante una clave privada, en particular la clave privada del fabricante del terminal, y por que la validez del segundo código de seguridad (22) cifrado es verificada por el algoritmo de autenticación multifactor (6) del terminal (4) mediante una clave pública (19), en particular la clave pública del fabricante del terminal.
8. Procedimiento según la reivindicación 7, caracterizado por que se determina un valor *hash* del primer código de seguridad (5) con ayuda de una función *hash* criptográfica que se aplica al primer código de seguridad (5) y por que la clave privada (20), en particular la clave privada del fabricante del terminal, se aplica a este valor *hash* del primer código de seguridad (5) para generar el segundo código de seguridad (22) en forma de una firma digital del primer código de seguridad (5).
9. Procedimiento según una de las reivindicaciones anteriores, caracterizado por que en el caso de un terminal móvil

del cliente, que constituye el segundo medio de almacenamiento (8), se instala en el terminal móvil una aplicación del proveedor, activada mediante el segundo código de seguridad (22), para la gestión de la unidad de control de gestión (3).

- 5 10. Sistema (1) para la puesta en servicio y la gestión de un dispositivo de control fuera de línea (2), en particular un dispositivo de control de acceso fuera de línea, mediante autenticación multifactor/ID, que comprende:

- un dispositivo de control (2) que presenta una unidad de control de gestión (3) y un terminal (4) que activa la unidad de control de gestión (3) con al menos una interfaz de datos (10, 11), en donde en el terminal (4) está implementado un algoritmo de autenticación multifactor/ID (6) y se pueden almacenar al menos un ID de autorización y un código de seguridad,
 - un primer medio de almacenamiento (7) móvil, en el que están almacenados a prueba de falsificaciones y de forma única para todo el mundo un ID de medio de almacenamiento y un primer código de seguridad (5),
 - un segundo medio de almacenamiento (8) móvil, en particular un terminal móvil, en el que está almacenado un segundo código de seguridad (22) generado con ayuda del primer código de seguridad (5),
- 10 en donde el algoritmo de autenticación multifactor/ID (6) para la puesta en servicio inicial del dispositivo de control (2) está programado para, en el caso de dos medios de almacenamiento (7, 8) colocados por un usuario en la ubicación del terminal, leer un ID de medio de almacenamiento y un código de seguridad (5) de uno de los medios de almacenamiento (7) y un código de seguridad (22) del otro medio de almacenamiento (8) mediante la al menos una interfaz de datos (10, 11) y verificar fuera de línea si el primer y el segundo código de seguridad (5, 22) leídos son mutuamente válidos y, de ser así, almacenar el ID de medio de almacenamiento como ID de autorización y el primer código de seguridad (5) en el terminal (4) y poner fin al modo de puesta en servicio inicial, y
- 15 en donde el algoritmo de autenticación multifactor/ID (6) para la gestión de la unidad de control de gestión (3) está programado para, en el caso de dos medios de almacenamiento colocados por un usuario en la ubicación del terminal, leer un ID de medio de almacenamiento y un código de seguridad de uno de los medios de almacenamiento y un código de seguridad del otro medio de almacenamiento mediante la al menos una interfaz de datos (10, 11) y verificar fuera de línea si el ID de medio de almacenamiento leído y el código de seguridad leído de uno de los medios de almacenamiento coinciden con el ID de autorización almacenado en el terminal (4) y con el primer código de seguridad (5) almacenado en el terminal (4) y si los dos códigos de seguridad (5, 22) leídos son mutuamente válidos, y, de ser así, activar la unidad de control de gestión (3) para la gestión por parte del usuario y poner fin al modo de gestión.

11. Sistema según la reivindicación 10, caracterizado por que el algoritmo de autenticación multifactor/ID (6) está programado para llevar a cabo la verificación de autenticación multifactor en el modo de gestión solo tras una verificación de autenticación de ID positiva.

12. Sistema según la reivindicación 10 u 11, caracterizado por que el algoritmo de autenticación multifactor/ID (6) está programado para activar la unidad de control de gestión (3) para la gestión de la unidad de control de gestión (3) por parte del usuario en el modo de puesta en servicio inicial tras almacenar el ID de autorización.

13. Sistema según una de las reivindicaciones 10 a 12, caracterizado por que el primer medio de almacenamiento (7) es un transpondedor, en particular un transpondedor RFID, y por que el terminal (4) presenta una interfaz de datos (10), en particular una interfaz RFID, para la lectura inalámbrica de los datos almacenados en el transpondedor.

14. Sistema según una de las reivindicaciones 10 a 13, caracterizado por que el segundo medio de almacenamiento (8) es un terminal móvil del cliente, en particular un teléfono inteligente, y por que el terminal (7) presenta una interfaz de datos (11), en particular una interfaz Bluetooth, para la lectura inalámbrica de los datos almacenados en el dispositivo móvil.

15. Sistema según una de las reivindicaciones 10 a 14, caracterizado por que el primer medio de almacenamiento (7) tiene protección contra copia/clonación, protección contra escritura, protección contra lectura y protección contra manipulación (15) y/o el segundo medio de almacenamiento (8) tiene protección contra manipulación (23).

16. Sistema según una de las reivindicaciones 10 a 15, caracterizado por que en un terminal móvil (8) del cliente está instalada una aplicación del proveedor, activada mediante el segundo código de seguridad (22), para la gestión de la unidad de control de gestión (3).

