(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 688 157**

(51) Int. CI.:

H04K 1/00 (2006.01)
H04L 29/06 (2006.01)
H04W 12/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.12.2014 E 14197821 (3)**

(97) Fecha y número de publicación de la concesión europea: **11.07.2018 EP 2887571**

(54) Título: **Caja de comunicación segura, conjunto de comunicación segura y método de comunicación segura asociado**

(30) Prioridad:

17.12.2013 FR 1302972

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
31.10.2018

(73) Titular/es:

ETAT FRANÇAIS REPRÉSENTÉ PAR LE DÉLÉGUÉ GÉNÉRAL POUR L'ARMEMENT, DGA/DS/SDPA/BPI (100.0%)
Bureau de la Propriété Intellectuelle, 60 Boulevard du Général Martial Valin, CS21623
Bureau de la Propriété Intellectuelle, FR

(72) Inventor/es:

COLAS, JEAN-BAPTISTE

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Caja de comunicación segura, conjunto de comunicación segura y método de comunicación segura asociado

[0001] La presente invención se refiere al campo de las telecomunicaciones, y en particular trata sobre una caja de interfaz de comunicación segura, un conjunto de comunicación segura y un método de comunicación segura asociado. El cifrado/descifrado de datos está experimentando un desarrollo significativo debido al crecimiento simultáneo del tráfico de datos y las velocidades de datos propuestas. De hecho, es importante proteger los datos y, de este modo, proteger las comunicaciones mediante operaciones de cifrado/descifrado para que los datos no se puedan leer ni utilizar si se interceptan.

[0002] Esto es especialmente cierto para las redes de comunicación inalámbricas que son más difíciles de proteger y en las que es más fácil interceptar los datos que se intercambian. En el ámbito militar, donde los datos intercambiados son aún más delicados, la protección de las comunicaciones mediante cifrado de datos es aún más crucial.

[0003] Existen muchos dispositivos para la comunicación segura mediante el cifrado de datos. En general, los dispositivos existentes proporcionan una comunicación cifrada entre dos dispositivos idénticos que tienen el mismo protocolo de cifrado/descifrado de datos usando un sistema de clave pública/clave privada, opcionalmente en combinación con certificados que identifican a los usuarios.

[0004] Por ejemplo, el dispositivo Nabishi NHT-78A de la empresa Nabishi Systems es una radio portátil que permite intercambios seguros entre dos o más usuarios equipados con el mismo dispositivo NHT-78A.

[0005] Un inconveniente de este dispositivo es que no permite la evolución de acuerdo con los estándares de telecomunicaciones.

[0006] Otro inconveniente es que es muy limitado en términos de interfaz de usuario, ya que permite principalmente la transmisión cifrada de datos de voz.

[0007] Del mismo modo, la solicitud de patente de los Estados Unidos US2005/0195667A1 divulga un dispositivo para inyectar datos de voz o datos digitales y que tiene una interfaz de usuario, que se puede usar para comunicarse con al menos otro dispositivo idéntico en cualquier tipo de red.

[0008] El inconveniente de este tipo de dispositivo es que no es evolutivo, y los medios de interfaz de usuario están limitados a los presentes en el dispositivo.

[0009] Por otra parte, se conoce la patente EP2106169 que describe una caja de interfaz de comunicación que comprende una interfaz de gestión, una fuente de alimentación eléctrica, un módulo de comunicación de corta distancia con un dispositivo portátil, controlado por la interfaz de gestión, un módulo de comunicación de larga distancia controlado por la interfaz de gestión y un módulo de cifrado/descifrado de comunicación de larga distancia, controlado por la interfaz de gestión. Este dispositivo tiene varios inconvenientes, incluyendo:

- La imposibilidad de transmitir progresivamente los datos de las otras cajas de interfaz de comunicación segura idénticas.
- la necesidad, en el dispositivo portátil, de la presencia de una puerta OR ausente en la mayoría de los dispositivos portátiles de consumo,
- la necesidad, para la transferencia de las claves de cifrado, de obtener o bien una conexión física entre el terminal principal y el dispositivo portátil (por ejemplo, un teléfono inteligente), o bien una transferencia física de la unidad de memoria.

[0010] Por lo tanto, existe el problema de que la rápida evolución de los diferentes medios de interfaz de usuario no se tiene en cuenta en estos dispositivos, por lo que una nueva interfaz de usuario requiere el diseño de un nuevo dispositivo.

[0011] La presente invención tiene como objetivo resolver los inconvenientes de la técnica anterior, proponiendo una caja capaz de asociarse por comunicación cifrada de corta distancia con cualquier dispositivo, en particular un teléfono móvil, un teléfono inteligente (también denominado más comúnmente *smartphone*), una tableta portátil, un ordenador, equipado con un medio de comunicación segura de corta distancia, y capaz de comunicarse de manera cifrada mediante comunicaciones de larga distancia con una caja idéntica, asociada a cualquier dispositivo equipado con un medio de comunicación segura de corta distancia.

[0012] La presente invención, al desplazar la comunicación de larga distancia a una caja separada, permite intercambiar directamente (*ad hoc*) datos por ondas de radio seguras en una capa baja material entre dos sistemas de comunicación móvil, sin que sea necesario tener en cuenta el modelo del sistema de comunicación

móvil.

[0013] Por lo tanto, la presente invención permite la transferencia segura de datos en una capa base material dentro de un conjunto heterogéneo de sistemas de comunicación móvil y, de este modo, permite la gestión de la obsolescencia programada de las interfaces de tipo teléfono inteligente.

[0014] La presente invención permite, entre dos o más cajas de interfaz de comunicación segura según la invención, una conexión de comunicación segura en una red de operador, o una conexión de comunicación segura directa sin una red centralizada (conexión de dispositivo a dispositivo o D2D) entre los dispositivos asociados con las cajas de interfaz de comunicación segura. El modo de comunicación retenido entre dos cajas de interfaz de comunicación segura es el túnel cifrado de punto a punto y de punto a multipuntos. Cada caja de interfaz de comunicación segura en modo D2D también puede transmitir los datos de otras cajas de interfaz de comunicación segura idénticas de manera progresiva.

[0015] Cuando la comunicación utiliza una red de operador, esta red puede ser una red móvil táctica (por ejemplo Auxylium®) o una red de telefonía móvil civil.

[0016] La caja de interfaz de comunicación segura de acuerdo con la invención puede comprender, en particular, sin que la invención se limite a este respecto, uno o más de:

- una placa base de soporte;
- un microsistema operativo NOR de tipo LINUX (marca registrada);
- un procesador de cálculo central (por ejemplo INTEL (marca registrada) (protegido) o ARM (marca registrada);
- un procesador de cálculo gráfico;
- una unidad de memoria RAM;
- una unidad de memoria NAND;
- un bus de gestión de radio;
- una antena de banda ancha 2G (GSM/GPRS/EDGE) y/o 3G (DC HSPA+ /HSPA+ /HSUPA /HSDPA /UMTS);
- una antena LTE (4G categoría 4 FDD/TDD);
- una antena Wi-Fi;
- una antena Bluetooth (marca registrada);
- una antena de GPS de alta sensibilidad (UHS);
- un conector de antena externa;
- una tarjeta SIM configurable;
- una tira de interfaz hombre/máquina (botón(es) y/o diodo(s) de emisión de luz);
- una batería extraíble de alta capacidad de tipo de iones de litio o de tecnología superior, accesible, por ejemplo, a través de una puerta de acceso formada en la caja de interfaz de comunicación segura;
- uno o más conectores micro-USB con un enlace de conexión específico.

[0017] El procesador de cálculo gráfico permite realizar, con el apoyo de los procesadores centrales, los procesos de cifrado y descifrado.

[0018] Las antenas de la caja de interfaz de comunicación segura de acuerdo con la invención están preferiblemente dentro de la caja por razones de volumen general de la caja pero también pueden, sin apartarse del alcance de la presente invención, ser externas, desmontables o no. Cada antena está asociada a un circuito de procesamiento de señales adecuado, también ubicado en la caja. Los bloques de procesamiento de señales pueden estar compartidos en uno o más bloques comunes a varias antenas.

[0019] La caja de interfaz de comunicación segura de acuerdo con la invención puede adoptar la forma de una carcasa de metal, preferiblemente de aluminio, cubierta con un revestimiento resistente a los golpes y antideslizante de caucho y plástico moldeado.

[0020] De acuerdo con una característica particular de la invención, la caja de interfaz de comunicación segura cumple con la norma IP57 en relación con el nivel de protección ofrecido por un dispositivo a las intrusiones de cuerpos sólidos y líquidos.

[0021] El interior de la caja de interfaz de comunicación segura puede equiparse con una placa disipadora de calor.

[0022] Ventajosamente, el peso de la caja de interfaz de comunicación segura no supera los 220 g con la batería, aunque la invención no está limitada a este respecto.

[0023] Ventajosamente, la caja de interfaz de comunicación segura según la invención puede tener dimensiones

que la hagan fácilmente transportable. La caja de interfaz de comunicación segura según la invención puede ser, por ejemplo, portátil y tener unas dimensiones de 130 mm de longitud, 80 mm de anchura y 28 mm de grosor, sin que la invención se limite a este respecto. Por lo tanto, puede tener sustancialmente las dimensiones y el tamaño de un teléfono móvil, ser liviana y, por lo tanto, fácilmente transportable por el usuario.

[0024] El cifrado puede usar claves gubernamentales validadas por la Agencia Nacional de Seguridad de Sistemas de Información, y consistir en el intercambio de claves simétricas después de un reconocimiento y una transferencia mediante claves asimétricas.

[0025] La caja de interfaz de comunicación segura es compatible con el modo de pila dual o dual stack IPv6/IPv4, pero la invención no se limita solo a este modo.

[0026] La caja de interfaz de comunicación segura puede comprender ventajosamente puertos de entrada/salida, por ejemplo, un enchufe para una antena externa, que se agregará a las antenas internas, y uno o más enchufes micro USB, utilizados, por ejemplo, para recargar la batería, una conexión por cable con el dispositivo portátil asociado o una conexión de mantenimiento.

[0027] La caja de interfaz de comunicación segura también puede incluir elementos de interfaz de usuario, tales como uno o más diodos emisores de luz o uno o más botones, en particular para verificar la asociación de la caja de interfaz de comunicación segura con un dispositivo portátil, su nivel de batería o para realizar el procedimiento de asociación con el dispositivo portátil.

[0028] La invención, por lo tanto, tiene por objeto una caja de interfaz de comunicación segura como se define en la reivindicación 1, y que comprende:

- una interfaz de gestión;
- una fuente de alimentación controlada por la interfaz de gestión;
- un módulo de comunicación de corta distancia con un dispositivo portátil, controlado por la interfaz de gestión;
- un módulo para cifrar/descifrar la comunicación de corta distancia entre la caja de interfaz de comunicación segura y el dispositivo portátil, controlado por la interfaz de gestión;
- un módulo de comunicación de larga distancia, controlado por la interfaz de gestión;
- un módulo de cifrado/descifrado de comunicación de larga distancia, controlado por la interfaz de gestión; y
- un módulo para calcular la posición de la caja de interfaz de comunicación segura, controlada por la interfaz de gestión.

[0029] La interfaz de gestión puede comunicarse con los diferentes módulos a través de uno o más buses de comunicación.

[0030] Los módulos descritos anteriormente son elementos funcionales que pueden implementarse en uno o más componentes de hardware, por ejemplo, uno o más procesadores, microprocesadores, microcontroladores, circuitos integrados para aplicaciones específicas (ASIC), matrices de puertas programables por el usuario (FPGA).

[0031] Como se ha indicado anteriormente, la batería puede ser una batería extraíble de alta capacidad del tipo de iones de litio o de tecnología superior, accesible, por ejemplo, a través de una puerta de acceso formada en la caja de interfaz de comunicación segura.

[0032] Por comunicación de corta distancia se entiende comunicaciones dentro de un radio de hasta tres metros entre el dispositivo portátil y la caja de interfaz de comunicación segura, que puede se asegurada por un cable que conecta el dispositivo portátil y la caja de interfaz de comunicación segura o una conexión inalámbrica de tipo Bluetooth® (por ejemplo) o cualquier otra tecnología de comunicación inalámbrica.

[0033] Por comunicación de larga distancia se hace referencia a a las comunicaciones inalámbricas entre una o más cajas de interfaz de comunicación segura, ya sea de manera directa o en cadena (D2D), o a través de una red telefónica móvil civil o táctica. De acuerdo con una forma de realización de la invención, el módulo de comunicación de corta distancia es un módulo de comunicación por estándar Bluetooth®, un módulo de comunicación por estándar Wi-Fi, un módulo de comunicación por estándar Wimax, un cable o una combinación de ellos.

[0034] La invención, sin embargo, no se limita a estos estándares y cualquier evolución de estos estándares o estándares futuros de comunicación de corta distancia se contempla en el contexto de la presente invención. El módulo de comunicación de corta distancia puede implementarse en forma de un chip con antena y medios de procesamiento de señales asociados, donde la antena preferiblemente está incorporada en la caja, pero también

puede ser externa, conectada a sus medios de procesamiento de señales asociados dentro de la caja.

[0035] Según una forma de realización de la invención, el módulo de comunicación de larga distancia es un módulo de comunicación según el estándar 2G, un módulo de comunicación según el estándar 3G, un módulo de comunicación según el estándar 4G civil, un módulo de comunicación según el estándar 4G fuera de banda, un módulo de comunicación según el estándar WIFI, un módulo de comunicación según el estándar Wimax, o una combinación de los mismos.

[0036] Sin embargo, la invención no está limitada a estos estándares, y cualquier evolución futura de estos estándares o nuevos estándares se considera dentro del alcance de la presente invención. Al igual que el módulo de comunicación de corta distancia, el módulo de comunicación de larga distancia puede implementarse en forma de un chip con antena y medios de procesamiento de señales asociados, donde la antena preferentemente está incorporada en la caja pero también puede ser externa, conectada a su medio de procesamiento de señales asociado en la caja.

[0037] De acuerdo con una forma de realización de la invención, el módulo de cálculo de posición es un sistema GPS civil, un sistema GPS de código Y, un sistema GLONASS, un sistema GALILEO, opcionalmente acoplado a un sistema GPS de código Y, o una combinación de uno o más de estos.

[0038] La invención, sin embargo, no se limita a estos sistemas, y cualquier evolución futura de estos sistemas o cualquier sistema nuevo se considera dentro del alcance de la presente invención. Este módulo también puede implementarse en forma de un chip de antena y medios de procesamiento de señal asociados, donde la antena preferiblemente está incorporada en la caja pero también puede ser externa, conectada a sus medios de procesamiento de señales asociados en la caja.

[0039] De acuerdo con una forma de realización de la invención, la interfaz de gestión comprende un sistema operativo incorporado. A modo de ejemplo, es posible prever un sistema operativo Linux (marca registrada) sin que la invención se vea limitada por ello.

[0040] De acuerdo con una forma de realización de la invención, la interfaz de gestión comprende un primer procesador a cargo de controlar los diversos elementos de la caja de interfaz de comunicación segura y el cifrado/descifrado de las comunicaciones de corta distancia y un segundo procesador a cargo del cifrado/descifrado de las comunicaciones de larga distancia.

[0041] Las formas de realización con un único procesador que ejecuta todas las tareas o con más de dos procesadores también se contemplan dentro del alcance de la presente invención.

[0042] Según una forma de realización de la invención, la caja de interfaz de comunicación segura comprende además un módulo de memoria, opcionalmente extraíble, que almacena las claves de cifrado/descifrado de las comunicaciones de corta distancia y las claves de cifrado/descifrado de las comunicaciones de larga distancia El módulo de memoria puede implementarse en forma de una tarjeta flash o una tarjeta SIM, o como una memoria integrada en un elemento de tipo procesador, microprocesador, microcontrolador, por ejemplo.

[0043] De acuerdo con una forma de realización de la invención, el módulo de memoria también almacena un certificado de autenticación del propietario de la caja de interfaz de comunicación segura. Ventajosamente, el módulo de memoria puede incluir varios certificados en caso de revocación después de una pérdida o robo.

[0044] De acuerdo con una forma de realización de la invención, cada módulo de comunicación de larga distancia comprende una antena correspondiente, estando dispuesta una pasta térmica en una capa de forma semitubular en la superficie interna de cada antena, estando dicha pasta térmica en contacto térmico en cada extremo de la antena con una pieza disipadora de calor que consiste en una alternancia de pasta térmica y metal (especialmente cobre), estando dicha parte disipadora de calor conectada térmicamente a una placa de disipación de calor dispuesta en la caja.

[0045] El contacto de la pasta térmica aplicada sobre la antena/de la pasta térmica aplicada sobre la placa de disipación de calor garantiza una disipación óptima del calor.

[0046] De acuerdo con una forma de realización de la invención, la caja consiste en una carcasa de metal, preferiblemente de aluminio, cubierta con un revestimiento antideslizante y resistente a los golpes, preferiblemente caucho y plástico moldeado.

[0047] Según una forma de realización de la invención, la caja comprende además uno o más puertos de entrada/salida controlados por la interfaz de gestión, por ejemplo puertos micro-USB, sin que la invención se limite a este tipo de puerto. Se pueden considerar otros tipos de puertos, por ejemplo, de tipo C, Lightning (marca registrada de Apple Inc.), Firewire (marca registrada) y cualquier desarrollo futuro de estos estándares o nuevos estándares.

[0048] De acuerdo con una forma de realización de la invención, la caja comprende además un módulo de extensión, que comprende un conector conectado a la interfaz de gestión mediante un bus de comunicación para un intercambio de señales de control y/o de datos con la interfaz de gestión. Se pueden citar como ejemplos de buses los buses de tipo miniPCI (marca registrada), M.2 de formato NGFF (Factor de forma de nueva generación), PCI-SIG (marca registrada) y cualquier evolución futura de estos estándares o nuevos estándares.

[0049] De acuerdo con una forma de realización de la invención, la caja de interfaz de comunicación segura comprende una caja de evolución adaptada para acceder a los otros módulos de la caja de interfaz de comunicación segura. El objeto de la invención es también un conjunto de comunicación segura como se define en la reivindicación 14. El objeto de la invención es también un método de comunicación segura como se define en la reivindicación 15.

[0050] Existen dos modos para generar claves y certificados: en el modo denominado centralizado (red de tipo estrella con un maestro y N esclavos), las claves se recuperan mediante la caja de interfaz de comunicación segura desde el maestro (servidor, ordenador, baliza de red) a partir del par de clave pública/clave privada y certificados (de tipo X.509 preferentemente, pero este formato no es exclusivo) previamente almacenadas en la caja de interfaz de comunicación segura. Este almacenamiento preliminar puede ser realizado por un administrador o por el usuario a través de un dispositivo de identificación (tarjeta RFID, medio de almacenamiento extraíble tal como una llave micro-USB o una tarjeta microSD (marca registrada). En el modo D2D, donde la generación de claves se puede realizar a través de una imagen o movimientos aleatorios en una pantalla, una caja maestra autodesignada distribuye las claves simétricas (el maestro puede cambiar según la reconfiguración de la red mediante la pérdida de la estación maestra inicial) gracias a las claves pública/privada y los certificados (preferiblemente de tipo OpenPGP, pero este formato no es exclusivo) previamente almacenados en las otras cajas. Este almacenamiento previo puede realizarlo un administrador o el usuario a través de un dispositivo de identificación (tarjeta RFID, soporte de almacenamiento extraíble, como una llave micro-USB o una tarjeta microSD (marca registrada) El sistema operativo del dispositivo portátil se puede virtualizar en la caja de interfaz de comunicación segura a la que está asociado, para controlar, a través de la interfaz de gestión de la caja de interfaz de comunicación segura, el dispositivo portátil, en particular su interfaz de usuario.

[0051] Para ilustrar mejor el objeto de la presente invención, se describirá a continuación una forma de realización preferida en referencia a los dibujos adjuntos.

[0052] En estos dibujos:

- La Figura 1 es un diagrama de bloques de una caja de interfaz de comunicación segura según la presente invención;
- La Figura 2 es un diagrama de bloques de un conjunto de comunicación segura de acuerdo con la presente invención;
- La figura 3 es un diagrama de bloques de un método de comunicación segura para recibir datos desde una caja de interfaz de comunicación segura en un modo de sistema operativo virtualizado;
- La figura 4 es un diagrama de bloques de un método de comunicación segura para transmitir datos desde una caja de interfaz de comunicación segura en un modo de sistema operativo virtualizado.
- La Figura 5 es un diagrama de bloques de un método de comunicación segura para recibir datos desde una caja de interfaz de comunicación segura en un modo de sistema operativo no virtualizado;
- La Figura 6 es un diagrama de bloques de un método para la comunicación segura de transmisión de datos desde una caja de interfaz de comunicación segura en un modo de sistema operativo no virtualizado.

[0053] En referencia a la Figura 1, se puede ver que se muestra una caja de interfaz de comunicación segura 1 de acuerdo con la presente invención.

[0054] La caja 1 de interfaz de comunicación segura comprende una interfaz de gestión 2, una fuente de alimentación 3, un módulo de comunicación de corta distancia 4, un módulo de cifrado/descifrado de comunicación de corta distancia 5, un módulo de comunicación de larga distancia 6, un módulo de cifrado/descifrado de la comunicación de larga distancia 7, un módulo de cálculo de posición 8 y un módulo de extensión 9.

[0055] La interfaz de gestión 2 de la caja de interfaz de comunicación segura 1 controla la fuente de alimentación 3, el módulo de comunicación de corta distancia 4, el módulo de cifrado/descifrado de la comunicación de corta distancia 5, el módulo de comunicación de larga distancia 6 , el módulo de cifrado/descifrado de la comunicación de larga distancia 7, el módulo de cálculo de posición 8 y el módulo de extensión 9.

[0056] El módulo de comunicación de corta distancia 4 se comunica con el módulo de cifrado/descifrado de la comunicación de corta distancia 5 y el módulo de comunicación de larga distancia 6 se comunica con el módulo de cifrado/descifrado de la comunicación de larga distancia 7.

[0057] El módulo de comunicación de corta distancia 4 es un módulo de comunicación por estándar Bluetooth®, un módulo de comunicación por estándar Wifi, un módulo de comunicación por estándar Wimax, un cable o una combinación de estos.

[0058] El módulo de comunicación de larga distancia 6 es un módulo de comunicación según el estándar 2G, un módulo de comunicación según el estándar 3G, un módulo de comunicación según el estándar 4G civil, un módulo de comunicación según el estándar 4G fuera de banda, un módulo de comunicación según el estándar Wifi (que también pertenece al módulo de comunicación de corta distancia 4), un módulo de comunicación Wimax (que también pertenece al módulo de comunicación de corta distancia 4), o una combinación de los mismos.

[0059] El módulo de cálculo de posición 8 es un sistema GPS civil, un sistema GPS de código Y, un sistema GLONASS, un sistema GALILEO, opcionalmente acoplado a un sistema GPS de código Y, o una combinación de uno o más de estos.

[0060] La caja de interfaz de comunicación segura 1 también incluye uno o más puertos de entrada/salida controlados por la interfaz de gestión 2.

[0061] El módulo de extensión 9 comprende un conector conectado a la interfaz de gestión 2 por un bus de comunicación para un intercambio de señales de control y/o de datos con la interfaz de gestión 2.
Por lo tanto, la caja de interfaz comprende, respecto a la patente EP2106169 :

- un módulo de cifrado/descifrado de la comunicación de corta distancia (5) entre la caja de interfaz de comunicación segura (1, 13, 14) y el dispositivo portátil (11, 12) controlado por la interfaz de gestión (2) que permite evitar la necesidad de que haya una puerta OR en el dispositivo portátil; por lo tanto, se implementan al menos dos procesadores para las acciones de cifrado/descifrado de manera que los datos se cifran de una manera diferente entre los dispositivos portátiles y su caja de interfaz de comunicación segura asociada, y entre las dos cajas de interfaz de comunicación segura.
- una fuente de alimentación eléctrica (3) controlada por la interfaz de gestión (2) y un módulo de cálculo de posición (8) de la caja de interfaz de comunicación segura (1, 13, 14), controlada por la interfaz de gestión (2) que permite no solo administrar la carga, la descarga de la fuente de alimentación, y la localización de la caja de interfaz, sino también asegurar la distribución de esta alimentación eléctrica a los componentes de la caja y desactivar la fuente de alimentación eléctrica y o dejarla permanentemente inoperativa a través de la acción de la interfaz de gestión sobre la fuente de alimentación eléctrica a partir de los elementos recopilados por el módulo de cálculo de posición, o inhabilitar, a partir de los elementos recopilados por el módulo de cálculo de posición, uno o más módulos de comunicación de la caja.

Por lo tanto, la interfaz de gestión de la caja de comunicación segura se basa en una arquitectura de software y hardware.
La arquitectura de hardware consiste en unidades de almacenamiento de memoria volátiles y no volátiles conectadas por señales eléctricas a puertas lógicas y en particular un módulo de cálculo digital que consiste en un procesador y un módulo de localización tal como un chip capaz de procesar la señal de GPS o GPRS. Los buses de comunicación permiten intercambios binarios entre la interfaz de gestión y los módulos de control de todos los módulos de la caja de comunicación segura. La arquitectura de software está compuesta en la versión virtualizada y no virtualizada del sistema operativo del terminal móvil asociado a la caja de interfaz de comunicación segura, una interfaz de firmware extensible unificada, una capa de abstracción de hardware, un sistema operativo con un núcleo que soporta en particular las funciones de control de la fuente de alimentación de los módulos de la caja de cifrado por conexión física con el módulo de gestión de energía. La interfaz de gestión tiene esquemas de reconocimiento cuyas huellas se almacenan al nivel del hardware en una memoria no regrabable o en una memoria regrabable. La interfaz de gestión consulta al nivel del software las huellas de los esquemas primarios y secundarios para compararlos con las huellas de los esquemas recibidos desde el módulo de localización, y el uno o más módulos de comunicación de larga distancia y corta distancia. Las informaciones que componen los esquemas primarios y secundarios son intervalos de posiciones geográficas de la caja de cifrado, el tipo de red en la que están conectados el módulo o módulos de comunicación de larga distancia, el tipo de terminal móvil asociado a través de los módulos de comunicación de corta distancia. Los esquemas primarios y secundarios se almacenan como una huella criptográfica. Los esquemas de destino se procesan para obtener un hash criptográfico a través de la interfaz de gestión a través de un algoritmo de software conectado al módulo de cálculo (procesador) y luego se compara en forma binaria con la huella de los esquemas primarios y secundarios. Si se determina que un esquema de destino es concordante, se habilita una rutina en el núcleo del sistema operativo y el código de arranque se escribe en paralelo a la raíz de la interfaz de firmware

extensible unificada adjunta al módulo de gestión. En este ejemplo, hay tres tipos de rutinas administradas por la interfaz de gestión denominadas ALM, COM y FLW a continuación para distinguirlas. Las rutinas ALM y COM no se pueden iniciar de forma independiente y la rutina COM siempre precede a la rutina ALM, excepto en el caso de un umbral de nivel de energía de la batería considerado demasiado bajo para garantizar el éxito de la rutina COM, en cuyo caso solo se activa la rutina ALM. La rutina FLW o COM y ALM también se puede activar según la hora del reloj suministrada y calibrada por la unidad de localización de la caja de interfaz de comunicación segura, duplicada por el reloj de 32 kHz del módulo de fuente de alimentación. En caso de desfase observado, este último módulo se referirá. La rutina COM inicia una secuencia de activación del código COM para cada uno de los firmware de los módulos de comunicación de larga distancia, y más particularmente el submódulo o módulos de amplificación de RF. Este código ejecuta por ejemplo en bucle una secuencia de transmisión de máxima potencia autorizada por el amplificador. La rutina COM hace que el módulo de comunicación de larga distancia permanezca inoperativo permanentemente al deteriorar por radiación térmica la integridad física de los componentes de hardware del amplificador de RF. La rutina ALM inicia una secuencia de activación del código ALM del firmware del módulo que asegura la distribución de la alimentación a los componentes de la caja. Este código causa un cortocircuito al invertir la definición de los polos del submódulo de gestión de la descarga de la batería. Esta secuencia induce un error en la batería e impide cualquier intento de alimentar la caja. La rutina FLW inicia una secuencia de activación del código FLX del firmware del módulo que asegura la distribución de la alimentación a los componentes de la caja y un código FLY de los firmware de los módulos de comunicación de larga distancia y corta distancia. La secuencia FLX induce una desactivación simple a través del canal VCI/OCP del canal de suministro del/de los amplificador(es) de RF, que puede(n) reactivarse restaurando el firmware a su configuración inicial. La secuencia FLY induce un desfase en las tablas de direccionamiento de memoria y de procesos de cálculo de las tramas de entrada y salida, pero no de las tramas de control, lo que hace que el o los módulos de destino no funcione(n).

[0062] La descripción dada anteriormente de los diferentes módulos solo es funcional, y los diferentes módulos pueden implementarse en uno o más componentes de hardware, sin apartarse del alcance de la presente invención.

[0063] En la práctica, la caja de interfaz de comunicación segura 1 consiste en una carcasa metálica, preferiblemente de aluminio, cubierta con un recubrimiento resistente a los golpes y antideslizante, preferiblemente hecho de caucho y plástico moldeado y que cumple con la norma IP57. Las antenas son preferiblemente internas respecto a la caja, pero también pueden ser externas, desmontables o no.

[0064] La disipación del calor generado por las antenas se puede realizar por medio de una pasta térmica dispuesta en una capa semitubular en la superficie interna de cada antena, estando dicha pasta térmica en contacto térmico en cada extremo de la antena con una parte disipadora de calor que consiste en una alternancia de pasta térmica y cobre, estando dicha parte disipadora de calor conectada térmicamente a una placa de disipación de calor dispuesta en la caja 1 de interfaz de comunicación segura.

[0065] En referencia a la figura 2, se puede ver que se muestra un conjunto de comunicación segura de acuerdo con la presente invención.

[0066] El conjunto de comunicación segura 10 comprende dos dispositivos portátiles 11, 12, dos cajas de interfaz de comunicación segura 13, 14 y una red de operador 17.

[0067] El primer dispositivo portátil 11 está asociado a la primera caja de interfaz de comunicación segura 13 y el segundo dispositivo portátil 12 está asociado a la segunda caja de interfaz de comunicación segura 14.

[0068] Los dispositivos portátiles 11, 12 se comunican de forma segura con sus respectivas cajas de interfaz de comunicación segura 13, 14 por comunicación cifrada de corta distancia 15 por medio del módulo de comunicación de corta distancia 4 y el módulo de cifrado/descifrado de comunicación de corta distancia 5 de las cajas de interfaz de comunicación segura 13, 14, como se describe con más detalle en referencia a las Figuras 3-6.

[0069] Las cajas de interfaz de comunicación segura 13, 14 son capaces de comunicarse mediante comunicación cifrada de larga distancia 16 por medio del módulo de comunicación de larga distancia 6 (o módulos WI-FI o Wimax del módulo de comunicación de corta distancia 4) y el módulo de cifrado/descifrado de comunicación de larga distancia 7 de las cajas de interfaz de comunicación segura 13, 14, directamente o a través de una red de operador 17.

[0070] El primer dispositivo portátil 11 puede comunicarse de forma segura con el segundo dispositivo portátil 12 mediante intercambio de datos entre el primer dispositivo portátil 11 y la primera caja de interfaz de comunicación segura 13 asociada mediante comunicación cifrada de corta distancia 15, intercambio de datos por comunicación de larga distancia cifrada 16 entre las dos cajas de interfaz de comunicación segura 13, 14, directamente o a través de una red de operador 17, y el intercambio de datos entre la segunda caja de interfaz de comunicación segura 14 y la segundo dispositivo portátil 12 por comunicación cifrada de corta distancia 15.

[0071] A su vez, el segundo dispositivo portátil 12 puede comunicarse de forma segura con el primer dispositivo portátil 11 mediante intercambio de datos entre el segundo dispositivo portátil 12 y la segunda caja de interfaz de comunicación segura 14 asociada por comunicación cifrada de corta distancia 15, intercambio de datos mediante comunicación cifrada de larga distancia 16 entre las dos cajas de interfaz de comunicación segura 13, 14, directamente o a través de una red de operador 17, y el intercambio de datos entre la primera caja de interfaz de comunicación segura 13 y el primer dispositivo portátil 11 por comunicación cifrada de corta distancia 15.

[0072] En aras de la simplicidad, solo se han mostrado dos dispositivos portátiles en la Figura 2, pero será evidente para los expertos en la técnica que puede haber un dispositivo emisor portátil y varios dispositivos receptores portátiles, sin alejarse del alcance y las enseñanzas de la presente invención. Asimismo, es posible transmitir de manera progresiva por medio de varias cajas de interfaz de comunicación segura.

[0073] De manera similar, en el diagrama donde hay varios dispositivos receptores portátiles, el dispositivo portátil emisor puede comunicarse con una parte de ellos mediante la vía caja de comunicación segura emisora-caja de comunicación segura receptora (conexión directa) y con otra parte de ellos por la vía caja de comunicación segura receptora- red operada- caja de comunicación segura receptora (conexión indirecta), sin apartarse del alcance y las enseñanzas de la presente invención.

[0074] En referencia a la figura 3, se puede ver que se muestra un método de comunicación segura de recepción de datos desde una caja de interfaz de comunicación segura en un modo de sistema operativo del dispositivo portátil virtualizado.

[0075] El método de comunicación segura de recepción de datos desde una caja de interfaz de comunicación segura 13 en un modo de sistema operativo virtualizado comprende un primer y segundo dispositivos portátiles 11, 12 de la figura 2, cada uno asociado respectivamente a un primer y segundo dispositivos portátiles 11, 12 de la Figura 2, y una segunda caja de interfaz de comunicación segura 13, 14.

[0076] La interfaz de gestión 2 de la caja de interfaz de comunicación segura 13 incluye un sistema operativo incorporado 18, un primer procesador 19, un segundo procesador 20 y un módulo de memoria 21.

[0077] El primer procesador 19 está a cargo de controlar los diversos elementos de la caja de interfaz de comunicación segura 13 y el cifrado/descifrado de las comunicaciones de corta distancia y el segundo procesador 20 está a cargo del cifrado/descifrado de las comunicaciones de larga distancia. Este ejemplo es solo ilustrativo, y los cálculos pueden distribuirse en uno o más procesadores en el contexto de la presente invención.

[0078] El módulo de memoria 21 es opcionalmente extraíble y almacena claves de cifrado/descifrado de corta distancia, claves de cifrado/descifrado de larga distancia y certificados de autenticación.

[0079] El método de comunicación segura para recibir datos desde una caja de interfaz de comunicación segura 13 en un modo de sistema operativo virtualizado, en el que el sistema operativo del primer dispositivo portátil 11 está virtualizado en el sistema operativo 18 de la primera caja de interfaz de comunicación segura 13, comprende: la recepción por la primera caja de interfaz de comunicación segura 13 de una señal de datos cifrada 22 desde la segunda caja de interfaz de comunicación segura 14 directamente o por medio de una red de operador 17, donde la señal de datos cifrados 22 es captada, desmodulada y luego convertida por el módulo de comunicación de larga distancia 6 de la primera caja de interfaz de comunicación segura 13 para luego ser enviada a la interfaz de gestión 2 de la primera caja de interfaz de comunicación segura 13, donde el sistema operativo 18 de la primera caja de interfaz de comunicación segura 13 controla permanentemente la interfaz de gestión 2 y el primer dispositivo portátil 11, asegurando así un retorno gráfico simple y de control al usuario; el descifrado de los datos recibidos 22 a través del segundo procesador 20 de la interfaz de gestión 2, recuperando el segundo procesador 20 una clave de lectura 23 del módulo de memoria 21 y verificando la validez del emisor a través de un certificado 24 también almacenado en el módulo de memoria 21; el procesamiento de los datos descifrados 25 por el sistema operativo 18, donde el sistema operativo 18 transfiere los datos 25 '(que pueden ser o no idénticos a los datos descifrados 25, dependiendo del tratamiento de los datos descifrados por el sistema operativo 18) al sistema operativo virtualizado 18 del primer dispositivo portátil 11; y el cifrado de una interacción de interfaz hombre-máquina por el primer procesador 19 con una clave de codificación 26 almacenada en el módulo de memoria 21, la firma de la interacción de la interfaz hombre-máquina con el certificado personal 27 del usuario almacenado en el módulo de memoria 21, y el envío de los datos cifrados 28 de la interacción de la interfaz hombre-máquina al módulo de comunicación de corta distancia 4 de manera que se transmitan al primer dispositivo portátil 11.

[0080] En referencia a la Figura 4, se puede ver que se muestra un método de comunicación segura de la transmisión de datos desde una caja de interfaz de comunicación segura en un modo de sistema operativo virtualizado.

[0081] El método de comunicación segura de transmisión de datos desde una caja de interfaz de comunicación segura 13 en un modo de sistema operativo virtualizado comprende un primer y segundo dispositivos portátiles 11, 12 de la Figura 2, cada uno asociado respectivamente a una primera y una segunda caja de interfaz de comunicación segura 13, 14.

[0082] La interfaz de gestión 2 de la caja de interfaz de comunicación segura 13 incluye un sistema operativo incorporado 18, un primer procesador 19, un segundo procesador 20 y un módulo de memoria 21.

[0083] El primer procesador 19 está a cargo de controlar los diversos elementos de la caja de interfaz de comunicación segura 13 y el cifrado/descifrado de las comunicaciones de corta distancia y el segundo procesador 20 está a cargo del cifrado/descifrado de las comunicaciones de larga distancia. El uso de al menos dos procesadores para las acciones de cifrado/descifrado permite:

- cifrar de manera diferente entre los dispositivos portátiles y su caja de interfaz de comunicación segura asociada, y entre las dos cajas de interfaz de comunicación segura,
- seleccionar un solo proceso criptográfico para cada uno de los enlaces entre los dispositivos portátiles y su caja de interfaz de comunicación segura asociada y un proceso común para los intercambios entre las cajas de interfaz de comunicación segura;
- una mejor gestión de los recursos de cálculo de la caja de cifrado mediante una asignación dinámica de la carga en función de los casos de uso de los usuarios. Por lo tanto, el tiempo de latencia en la transmisión de información se puede controlar mejor y reducir;
- una mayor solidez del modelo criptográfico porque la pérdida de un dispositivo portátil asociado a la caja de interfaz de comunicación segura no da como resultado que se comprometa el proceso de cifrado entre las cajas de interfaz de comunicación segura;
- en el plano físico, obtener una mejor distribución de la disipación de calor en la caja de interfaz de comunicación segura mediante una distribución espacial de las unidades de cálculo teniendo en cuenta una separación física de los procesadores útil para un menor aumento de la temperatura del conjunto del dispositivo. Por lo tanto, se controla el desgaste prematuro de los componentes, así como un mejor uso de los recursos de cálculo mediante una mayor disponibilidad de los componentes y su capacidad para mantener una alta frecuencia de reloj a lo largo del tiempo.

[0084] El módulo de memoria 21 es opcionalmente extraíble y almacena claves de cifrado/descifrado de corta distancia, claves de cifrado/descifrado de larga distancia y certificados de autenticación.

[0085] El método de comunicación segura de transmisión de datos desde una caja de interfaz de comunicación segura 13 en un modo de sistema operativo virtualizado, en el que el sistema operativo del primer dispositivo portátil 11 está virtualizado en el sistema operativo 18 de la primera caja de interfaz de comunicación segura 13, comprende: la recepción por la primera caja de interfaz de comunicación segura 13 de una señal de datos cifrados 29 (datos de control o datos procedentes de los sensores del dispositivo portátil 11 tales como imágenes, sonidos, ...) desde el primer dispositivo portátil 11, la señal de datos cifrados 29 es recogida, desmodulada y luego convertida por el módulo de comunicación de corta distancia 4 de la primera caja de interfaz de comunicación segura 13 para luego ser enviada a la interfaz de gestión 2 de la primera caja de interfaz de comunicación segura 13; el descifrado de los datos recibidos 29 a través del primer procesador 19 de la interfaz de gestión 2, recuperando el primer procesador 19 una clave de lectura 30 del módulo de memoria 21 y verificando la validez del emisor a través de un certificado personal 27 también almacenado en el módulo de memoria 21; el procesamiento de los datos descifrados 31 por el sistema operativo 18, donde el sistema operativo 18 los transfiere al sistema operativo virtualizado 18 del primer dispositivo portátil 11; el sistema operativo virtualizado 18 puede entonces, si es necesario, enviar datos 31’ a través del cifrado por el segundo procesador 20 con una clave de codificación 32 almacenada de control 31' con el certificado personal 27 almacenado en el módulo de memoria 21 y el envío de los datos cifrados 33 al módulo de comunicación de larga distancia 6 de manera que se transmitan a la segunda caja de interfaz de comunicación segura 14 directamente o a través de una red de operador 17.

[0086] En referencia a la figura 5, se puede ver que se representa un método de comunicación segura para recibir datos desde una caja de interfaz de comunicación segura en un modo de sistema operativo no virtualizado.

[0087] El método de comunicación segura de recepción de datos desde una caja de interfaz de comunicación segura 13 en un modo de sistema operativo no virtualizado comprende un primer y segundo dispositivos portátiles 11, 12 de la figura 2, cada uno asociado respectivamente a una primera y una segunda caja de interfaz de comunicación segura 13, 14.

[0088] La interfaz de gestión 2 de la caja de interfaz de comunicación segura 13 incluye un sistema operativo incorporado 18, un primer procesador 19, un segundo procesador 20 y un módulo de memoria 21.

[0089] El primer procesador 19 está a cargo de controlar los diversos elementos de la caja de interfaz de comunicación segura 13 y del cifrado/descifrado de las comunicaciones de corta distancia y el segundo procesador 20 está a cargo del cifrado/descifrado de las comunicaciones de larga distancia.

[0090] El módulo de memoria 21 es opcionalmente extraíble y almacena claves de cifrado/descifrado de corta distancia, claves de cifrado/descifrado de larga distancia y certificados de autenticación.

[0091] El método de comunicación segura para la recepción de datos desde una caja de interfaz de comunicación segura 13 en un modo de sistema operativo no virtualizado comprende: la recepción por la primera caja de interfaz de comunicación segura 13 de una señal de datos 22 desde la segunda caja de interfaz de comunicación segura 14 directamente o a través de una red de operador 17, donde la señal de datos cifrados 22 es recogida, desmodulada y luego convertida por el módulo de comunicación de larga distancia 6 de la primera caja de interfaz de comunicación segura 13 para luego ser enviada a la interfaz de gestión 2 de la primera caja de interfaz de comunicación segura 13; el descifrado de los datos recibidos 22 a través del segundo procesador 20 de la interfaz de gestión 2, recuperando el segundo procesador 20 una clave de lectura 23 del módulo de memoria 21 y verificando la validez del emisor a través de un certificado 24 también almacenado en el módulo de memoria 21; la transmisión de los datos descifrados al primer procesador 19; el cifrado de los datos descifrados recibidos por el primer procesador 19 usando una clave de codificación 26 almacenada en el módulo de memoria 21 y un certificado personal 27 del usuario almacenado en el módulo de memoria 21; y el envío de los datos cifrados 28 al módulo de comunicación de corta distancia 4 para su transmisión al primer dispositivo portátil 11.

[0092] En referencia a la Figura 6, se puede ver que se representa un método de comunicación segura de transmisión de datos desde una caja de interfaz de comunicación segura en un modo de sistema operativo no virtualizado.

[0093] El método de comunicación segura de transmisión de datos desde una caja de interfaz de comunicación segura 13 en un modo de sistema operativo no virtualizado incluye un primer y segundo dispositivos portátiles 11, 12 asociados cada uno respectivamente a una primera y una segunda caja de interfaz de comunicación segura 13, 14.

[0094] La interfaz de gestión 2 de la caja de interfaz de comunicación segura 13 incluye un sistema operativo incorporado 18, un primer procesador 19, un segundo procesador 20 y un módulo de memoria 21.

[0095] El primer procesador 19 está a cargo de controlar los diversos elementos de la caja de interfaz de comunicación segura 13 y el cifrado/descifrado de las comunicaciones de corta distancia y el segundo procesador 20 está a cargo del cifrado/descifrado de las comunicaciones de larga distancia.

[0096] El módulo de memoria 21 es opcionalmente extraíble y almacena claves de cifrado/descifrado de corta distancia, claves de cifrado/descifrado de larga distancia y certificados de autenticación.

[0097] El método de comunicación segura de transmisión de datos desde una caja de interfaz de comunicación segura 13 en un modo de sistema operativo no virtualizado comprende: la recepción por la primera caja de interfaz de comunicación segura 13 de una señal datos cifrados 29 del primer dispositivo portátil 11, donde la señal de datos cifrados 29 es recogida, desmodulada y luego convertida por el módulo de comunicación de corta distancia 4 de la primera caja de interfaz de comunicación segura 13 para luego ser enviada a la interfaz de gestión 2 de la primera caja 13 de interfaz de comunicación segura; el descifrado de los datos recibidos 29 a través del primer procesador 19 de la interfaz de gestión 2, recuperando el primer procesador 19 una clave de lectura 30 del módulo de memoria 21 y verificando la validez del emisor a través de un certificado personal 27 también almacenado en el módulo de memoria 21; la transmisión de los datos descifrados 31 al segundo procesador 20; y el cifrado de los datos 31 por el segundo procesador 20 con una clave de codificación 32 almacenada en el módulo de memoria 21, la firma de los datos 31 con el certificado personal 27 almacenado en el módulo de memoria 21 y el envío de los datos cifrados 33 al módulo de comunicación de larga distancia 6, de modo que se transmitan a la segunda caja de interfaz de comunicación segura 14 directamente o a través de una red de operador 17.

[0098] Los elementos secretos de la caja de la interfaz de comunicación segura se almacenan en una memoria extraíble con las claves simétricas de cifrado y descifrado correspondientes a los algoritmos de los procesadores y los certificados de autenticación de los diferentes interlocutores remotos. Una tarjeta SIM almacena el certificado de autenticación personal del titular de la caja de interfaz de comunicación segura. Este mismo certificado personal se almacena en el dispositivo portátil asociado a la caja de interfaz de comunicación segura. La misma tarjeta SIM puede almacenar varios certificados para gestionar el problema de la revocación por pérdida o robo de cajas de interfaz de comunicación segura y remotas.

[0099] El indicador de tiempo de la caja de interfaz de comunicación segura es particularmente útil para las acciones de cifrado y descifrado. El indicador de tiempo viene dado por la señal GPS recibida a través de los circuitos de procesamiento de señal de las antenas de cálculo de posición (GPS) o a través de un reloj maestro

del maestro de red. Los conjuntos GPS también alimentan la posición del usuario que se transmite al dispositivo portátil (configuración no virtualizada) o se recupera mediante el sistema operativo interno para integrarse con el sistema operativo virtualizado de la caja de interfaz de comunicación segura (configuración virtualizada).

[0100] La asociación entre la caja de interfaz de comunicación segura y su dispositivo portátil asociado se establece gracias a los certificados compartidos en cada una de las tarjetas SIM (tarjeta SIM del dispositivo portátil y tarjeta SIM de la caja de interfaz de comunicación segura) y una autenticación por diferentes medios estándar (código de acceso, código PIN ...) o una autenticación fuerte si el dispositivo portátil está equipado (huella digital, reconocimiento facial, reconocimiento de voz ...). Es el protocolo Bluetooth® o la conexión de cable el que soportará el intercambio de datos para que coincida con los dos dispositivos. La conexión por cable puede sustituir a la conectividad Bluetooth® en caso de perturbaciones electromagnéticas (interferencias, etc.).

[0101] Con el fin de proporcionar una interacción entre la caja de interfaz de comunicación segura y el usuario, toda la información del nivel de la batería o las fallas del sistema se retransmiten al dispositivo portátil. Un LED y un botón también se integran en la caja de interfaz de comunicación segura y son administrados por el sistema operativo interno de la caja de interfaz de comunicación segura para proporcionar los elementos esenciales como el nivel de batería, carga del sistema, o su asociación.

[0102] La fuente de alimentación de energía de todos los componentes de la caja de interfaz de comunicación segura es proporcionada por una batería equipada con un módulo de gestión que permite optimizar la carga y descarga de la batería.

[0103] Con el fin de alimentar la batería y cargarla, se puede conectar una fuente de alimentación externa a la caja de interfaz de comunicación segura mediante conectores. La gestión de la carga y la protección contra sobretensiones se proporcionan a través del bus de gestión de la batería.

[0104] En el modo de red móvil operada, las claves de cifrado simétricas para procesadores y los certificados de usuario se almacenan en uno o más servidores de referencia. El certificado de autenticación personal permite al usuario, a partir de un par de claves asimétricas privada/pública, recibir remotamente la lista de claves y certificados en tiempo real. Este dispositivo también permite revocar de la red a los usuarios que han puesto en peligro su caja de interfaz de comunicación segura. Entonces, en comparación con la patente EP2106169, la invención no requiere, para la transferencia de las claves de cifrado, obtener o bien una conexión física entre el terminal principal y el dispositivo portátil (por ejemplo, un *smartphone*) o bien una transferencia física de la unidad de memoria.

[0105] La implementación del software de la caja de interfaz de comunicación segura interviene o bien mediante la conexión de un cable perteneciente a un sistema informático autorizado y conectado a uno de los puertos de la caja de interfaz de comunicación segura, o bien a través de la red móvil operada que propaga los datos de configuración desde un servidor dedicado. Los intercambios se cifran y descifran a través del procesador o los procesadores en la caja de interfaz de comunicación segura en la que las claves de cifrado y lectura se inyectan con los certificados almacenados en la memoria.

[0106] Además, se puede proporcionar un espacio de evolución, que puede acomodar un módulo externo que pueda llevar una tecnología aún no desarrollada. Este complemento puede acceder a los otros módulos de la caja de interfaz de comunicación segura.

REIVINDICACIONES

1. Caja de interfaz de comunicación segura (1, 13, 14), que comprende:

- una interfaz de gestión (2);
- una fuente de alimentación eléctrica (3) controlada por la interfaz de gestión (2);
- un módulo de comunicación de corta distancia (4) con un dispositivo portátil (11, 12), controlado por la interfaz de gestión (2);
- un módulo de cifrado/descifrado de la comunicación de corta distancia (5) entre la caja de interfaz de comunicación segura (1, 13, 14) y el dispositivo portátil (11, 12), controlado por la interfaz de gestión (2);
- un módulo de comunicación de larga distancia (6), controlado por la interfaz de gestión (2);
- un módulo de cifrado/descifrado de la comunicación de larga distancia (7), controlado por la interfaz de gestión (2);
- un módulo para calcular la posición (8) de la caja de interfaz de comunicación segura (1, 13, 14), controlado por la interfaz de gestión (2); y

donde la caja de interfaz de comunicación segura (1, 13, 14) **se caracteriza por el hecho de que** está adaptada de tal manera que permite que:

- la fuente de alimentación (3) se desactive y/o se vuelva definitivamente inoperativa mediante la acción de la interfaz de gestión (2) en la fuente de alimentación (3) a partir de los elementos recogidos por el módulo de cálculo de posición (8), o
- al menos uno de los módulos de comunicación (4, 6) de la caja (1, 13, 14) se vuelve inoperativo a partir de los elementos recogidos por el módulo de cálculo de posición (8).

2. Caja de interfaz de comunicación segura (1, 13, 14) según la reivindicación 1, **caracterizada por el hecho de que** el módulo de comunicación de corta distancia (4) es un módulo de comunicación según el estándar Bluetooth®, un módulo de comunicación según el estándar Wifi, un módulo de comunicación según el estándar Wimax, un cable o una combinación de los mismos.

3. Caja de interfaz de comunicación segura (1, 13, 14) según la reivindicación 1 o la reivindicación 2, **caracterizada por el hecho de que** el módulo de comunicación de larga distancia (6) es un módulo de comunicación según el estándar 2G, un módulo de comunicación según el estándar 3G, un módulo de comunicación según el estándar 4G civil, un módulo de comunicación según el estándar 4G fuera de banda, un módulo de comunicación según el estándar WIFI, un módulo de comunicación según el estándar Wimax, o una combinación de los mismos.

4. Caja de interfaz de comunicación segura (1, 13, 14) según una de las reivindicaciones 1 a 3, **caracterizada por el hecho de que** el módulo de cálculo de posición (8) es un sistema GPS civil, un sistema GPS de código Y, un sistema GLONASS, un sistema GALILEO, un sistema GALILEO acoplado a un sistema GPS de código Y, o una combinación de uno o más de los mismos.

5. Caja interfaz de comunicación segura (1, 13, 14) según una de las reivindicaciones 1 a 4, **caracterizada por el hecho de que** la interfaz de gestión (2) comprende un sistema operativo integrado (18).

6. Caja de interfaz de comunicación segura (1, 13, 14) según una de las reivindicaciones 1 a 5, **caracterizada por el hecho de que** la interfaz de gestión (2) comprende un primer procesador (19) que se encarga de controlar los diferentes elementos de la caja de interfaz de comunicación segura (1, 13, 14) y del cifrado/descifrado de las comunicaciones de corta distancia y un segundo procesador (20) que se encarga del cifrado/descifrado de las comunicaciones de larga distancia.

7. Caja de interfaz de comunicación segura (1, 13, 14) según una de las reivindicaciones 1 a 6, **caracterizada por el hecho de que** comprende además un módulo de memoria (21) o un módulo de memoria extraíble, que almacena las claves de cifrado/descifrado (26, 30) de las comunicaciones de corta distancia y las claves de cifrado/descifrado (23, 32) de las comunicaciones de larga distancia.

8. Caja de interfaz de comunicación segura según la reivindicación 7, **caracterizada por el hecho de que** el módulo de memoria almacena adicionalmente un certificado de autenticación (24, 27) del titular de la caja de interfaz de comunicación segura (1, 13, 14).

9. Caja de interfaz de comunicación segura (1, 13, 14) según una de las reivindicaciones 1 a 8, **caracterizada por el hecho de que** cada módulo de comunicación de larga distancia (6) comprende una antena correspondiente, estando dispuesta una pasta térmica en una capa de forma semitubular en la superficie interna de cada antena, estando dicha pasta térmica en contacto térmico en cada extremo de la antena con una pieza

disipadora de calor constituida por una alternancia de pasta térmica y metal, estando dicha parte disipadora de calor conectada térmicamente a una placa disipadora de calor dispuesta en la caja.

10. Caja de interfaz de comunicación segura (1, 13, 14) según una de las reivindicaciones 1 a 9, **caracterizada por el hecho de que** comprende una carcasa de metal recubierta con un revestimiento resistente a los golpes y antideslizante.

11. Caja de interfaz de comunicación segura (1, 13, 14) según una de las reivindicaciones 1 a 10, **caracterizada por el hecho de que** comprende además uno o más puertos de entrada/salida controlados por la interfaz de gestión (2).

12. Caja de interfaz de comunicación segura (1, 13, 14) según una de las reivindicaciones 1 a 11, **caracterizada por el hecho de que** comprende además un módulo de extensión (9), que comprende un conector conectado a la interfaz de gestión (2) por un bus de comunicación para intercambiar señales de control y/o datos con la interfaz de gestión (2).

13. Caja de interfaz de comunicación segura (1, 13, 14) según una de las reivindicaciones 1 a 12, **caracterizada por el hecho de que** comprende una caja de evolución adaptada para acceder a los otros módulos de la caja de interfaz de comunicación segura.

14. Conjunto de comunicación segura (10), que comprende dos dispositivos portátiles (11, 12) y dos cajas de interfaz de comunicación segura (1, 13, 14) según cualquiera de las reivindicaciones 1 a 12, estando asociado cada uno de los dos dispositivos portátiles con una de las dos cajas de interfaz de comunicación segura (1, 13, 14) y comunicado de forma segura con esta a través de comunicación cifrada por medio de los módulos de comunicación de corta distancia (4) y de cifrado/descifrado de comunicaciones de corta distancia (5), donde las dos cajas de interfaz de comunicación segura (1, 13, 14) están adaptadas para comunicarse a través de comunicación cifrada de larga distancia mediante módulos de comunicación de larga distancia (6) y de cifrado/descifrado de comunicación de larga distancia (7), donde los dispositivos portátiles (11, 12) se comunican de forma segura por intercambio de datos entre el dispositivo portátil (11, 12) emisor y su caja de interfaz de comunicación segura (1, 13, 14) asociada por comunicación cifrada de corta distancia, intercambio de datos a través de comunicación cifrada de larga distancia entre las dos cajas de interfaz de comunicación segura (1, 13, 14) e intercambio de datos entre la caja de interfaz de comunicación segura (1, 13, 14) asociada al dispositivo portátil (11, 12) receptor y el dispositivo portátil (11, 12) receptor a través de comunicación cifrada de corta distancia, donde los datos se cifran/descifran en cada caja de interfaz de comunicación segura (1, 13, 14) de manera que los datos se cifran de forma diferente entre los dispositivos portátiles (11, 12) y su caja de interfaz de comunicación segura asociada (1, 13, 14), y entre las dos cajas de interfaz de comunicación segura (1, 13, 14).

15 Método de comunicación segura dentro de un conjunto de comunicación segura (10) según la reivindicación 14, conjunto en el que uno de los dispositivos portátiles (11, 12), denominado dispositivo portátil emisor, está asociado a una de las cajas de interfaz de comunicación segura (1, 13, 14), denominada caja emisora, y en el que al menos otro de los dispositivos portátiles (11, 12), denominado dispositivo portátil receptor, está asociado cada uno a otra de las cajas de interfaz de comunicación segura (1, 13, 14), denominada caja receptora, método que comprende:

- la generación de datos en el dispositivo portátil emisor (11, 12);
- el cifrado de datos en el dispositivo portátil emisor (11, 12);
- el envío de los datos cifrados desde el dispositivo portátil (11, 12) emisor a la caja emisora por comunicación de corta distancia;
- el descifrado de los datos cifrados por medio de una clave de lectura (30) y de un certificado personal (27) situados en el módulo de memoria (21) de la caja emisora;
- el cifrado de los datos descifrados por medio de una clave de codificación (32) y de un certificado personal (27) situados en el módulo de memoria (21) de la caja emisora;
- el envío de los datos así cifrados a una o más cajas receptoras por comunicación de larga distancia;

y en cada caja receptora:

- el descifrado de los datos cifrados por medio de una clave de lectura (23) y de un certificado personal (24) ubicados en el módulo de memoria (21) de la caja receptora;
- el cifrado de los datos descifrados por medio de una clave de codificación (26) y de un certificado personal (27) ubicados en el módulo de memoria (21) de la caja receptora;
- el envío de los datos así cifrados al dispositivo portátil receptor (11, 12) por comunicación de corta distancia;
- el descifrado de los datos cifrados por el dispositivo portátil receptor (11, 12); estando el sistema operativo del dispositivo portátil (11, 12) virtualizado en la caja de interfaz de comunicación segura (1, 13, 14) a la que está asociado, para controlar, por medio de la interfaz de gestión (2) de la caja de interfaz de comunicación segura (1, 13, 14), el dispositivo portátil (11, 12).

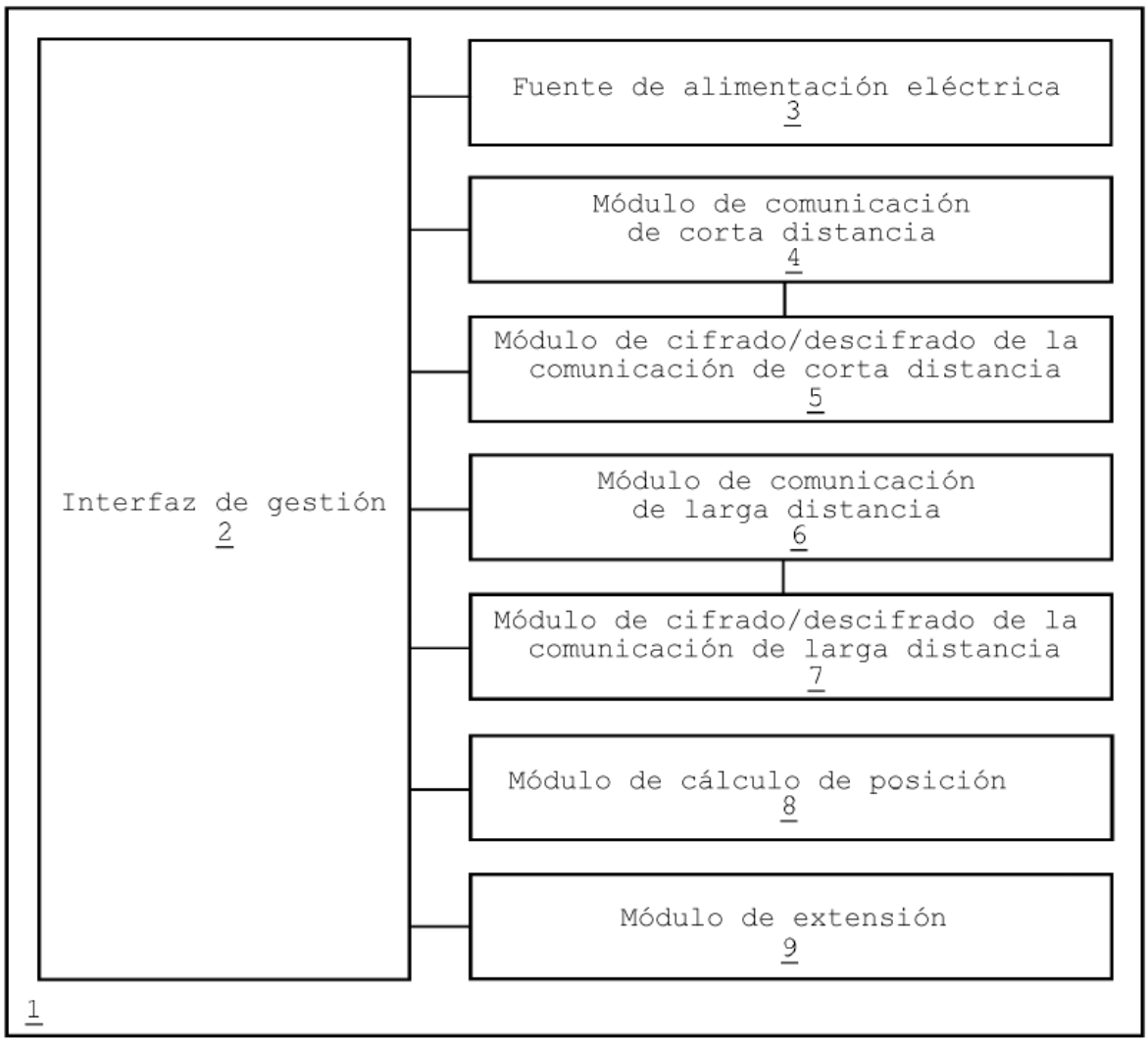
Interfaz de gestión
2
Fuente de alimentación eléctrica
3
Módulo de comunicación
de corta distancia
4
Módulo de cifrado/descifrado de la
comunicación de corta distancia
5
Módulo de comunicación
de larga distancia
6
Módulo de cifrado/descifrado de la
comunicación de larga distancia
7
Módulo de cálculo de posición
8
Módulo de extensión
9
1

FIGURA 1

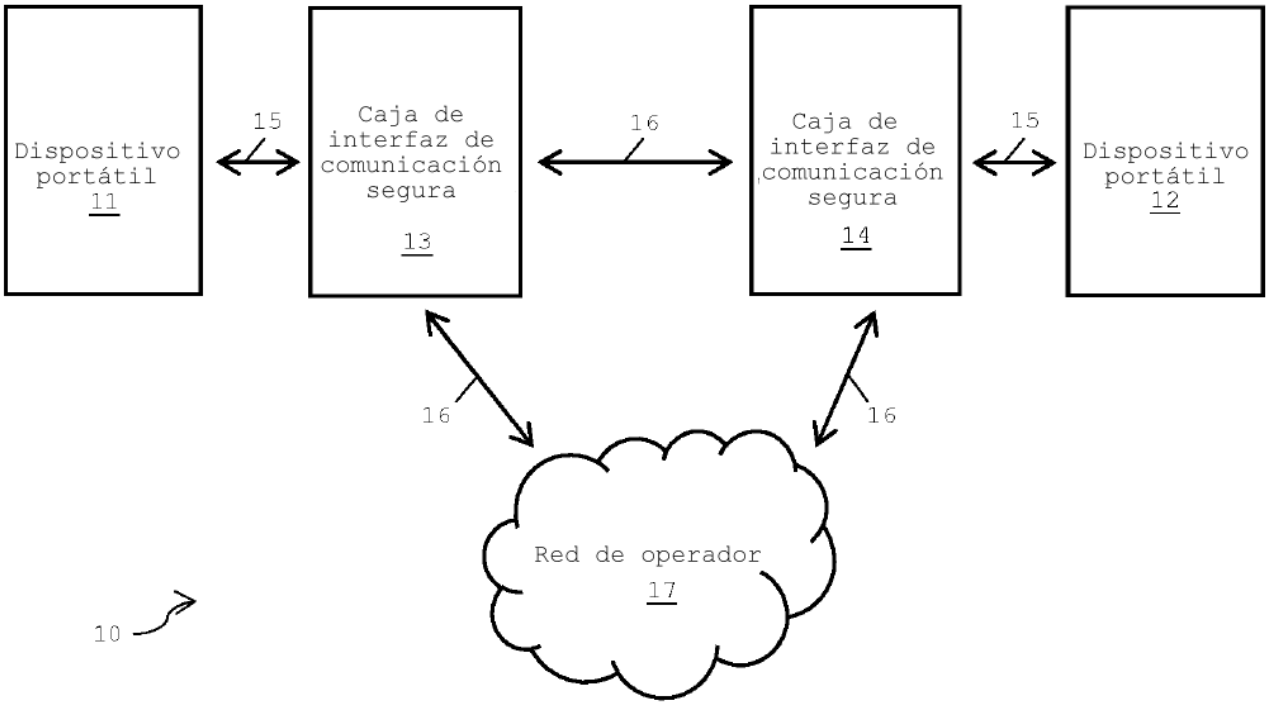
Dispositivo portátil 11
15
Caja de interfaz de comunicación segura 13
16
Caja de interfaz de comunicación segura 14
15
Dispositivo portátil 12
16
16
Red de operador 17
10

FIGURA 2

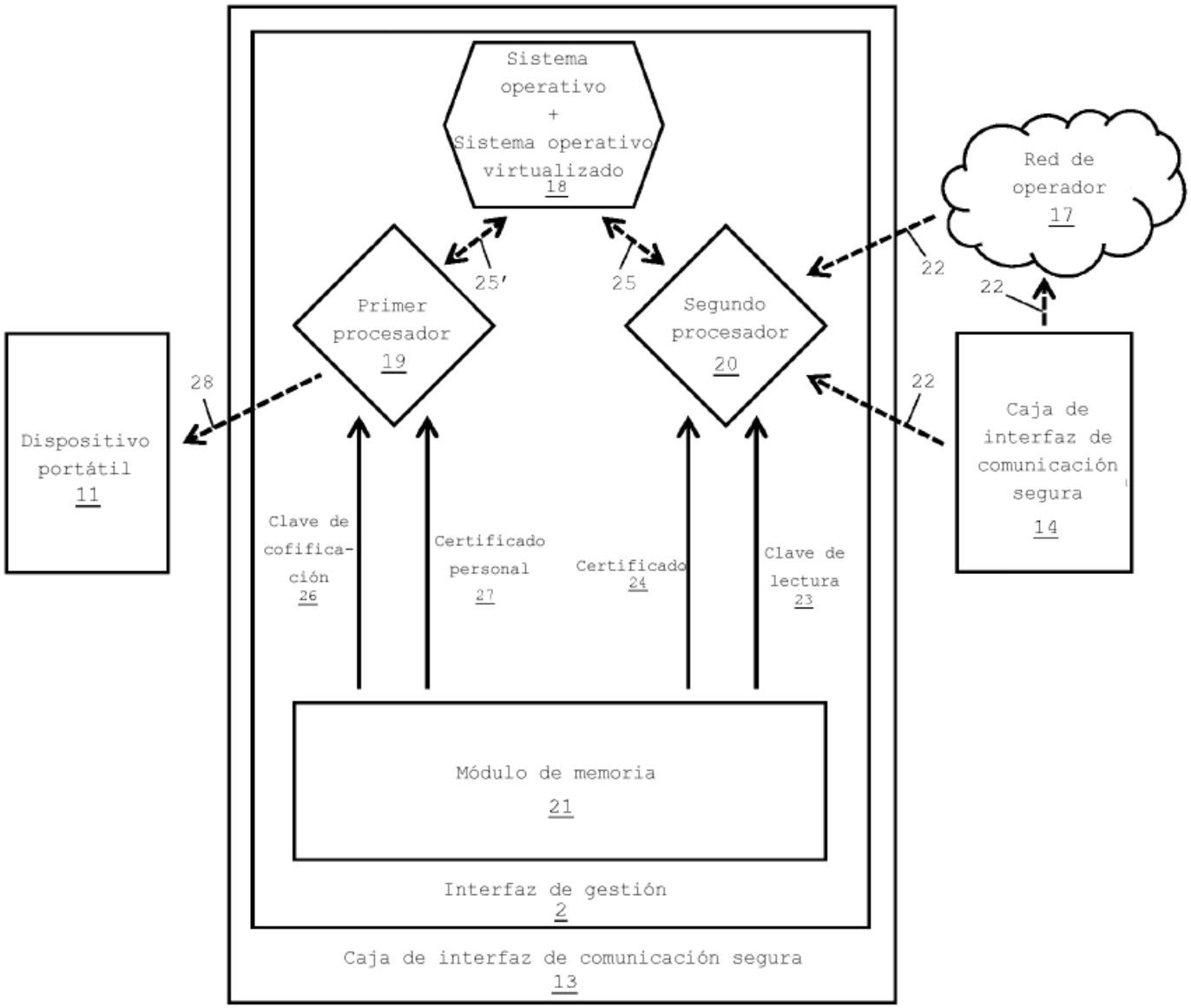
Sistema operativo + Sistema operativo virtualizado 18
Red de operador 17
25'
25
22
22
Primer procesador 19
Segundo procesador 20
28
22
Dispositivo portátil 11
Caja de interfaz de comunicación segura 14
Clave de cofificación 26
Certificado personal 27
Certificado 24
Clave de lectura 23
Módulo de memoria 21
Interfaz de gestión 2
Caja de interfaz de comunicación segura 13

FIGURA 3

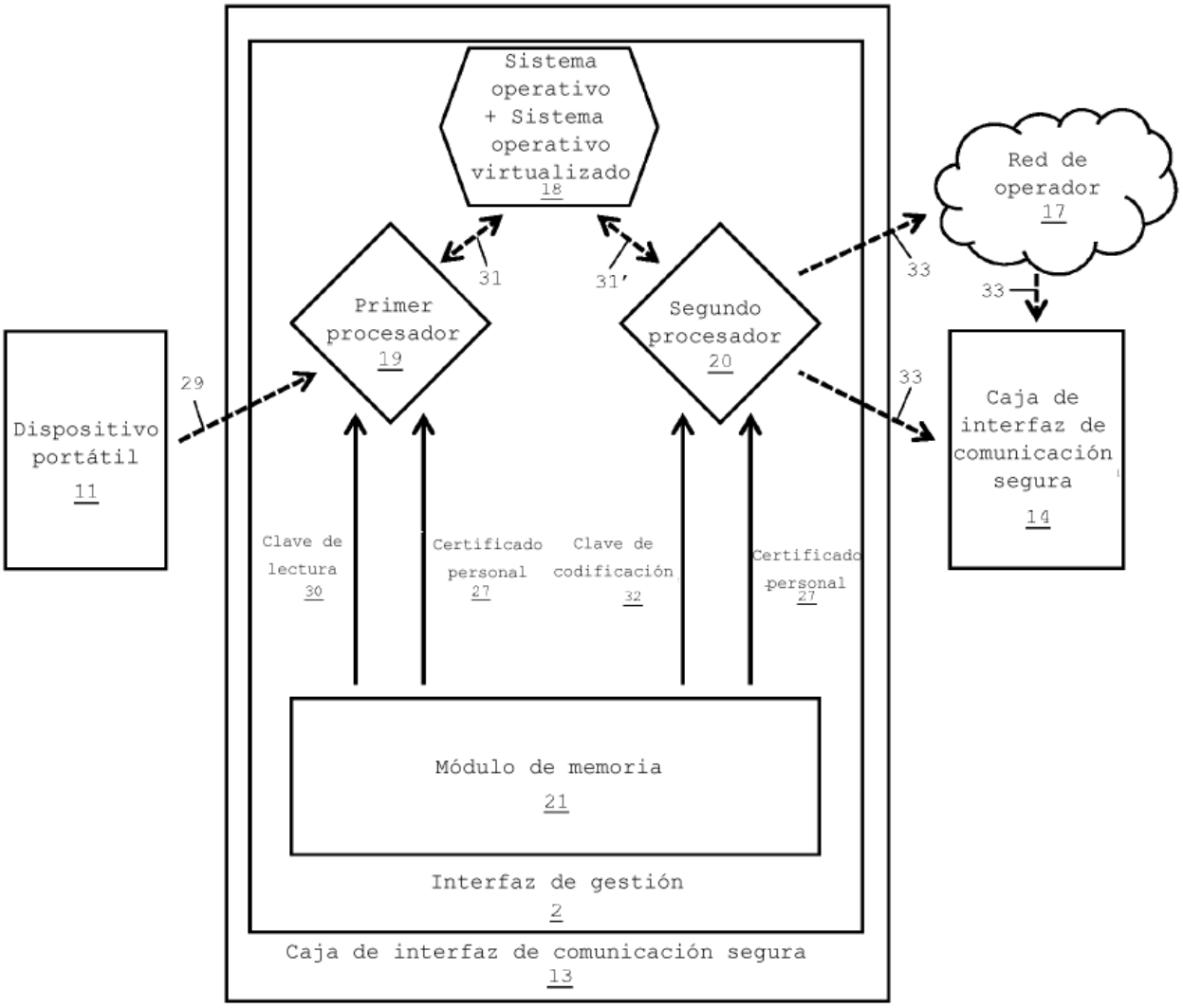
Sistema operativo + Sistema operativo virtualizado
18
Red de operador
17
31
31'
33
33
Primer procesador
19
Segundo procesador
20
Dispositivo portátil
11
29
33
Caja de interfaz de comunicación segura
14
Clave de lectura
30
Certificado personal
27
Clave de codificación
32
Certificado personal
27
Módulo de memoria
21
Interfaz de gestión
2
Caja de interfaz de comunicación segura
13

FIGURA 4

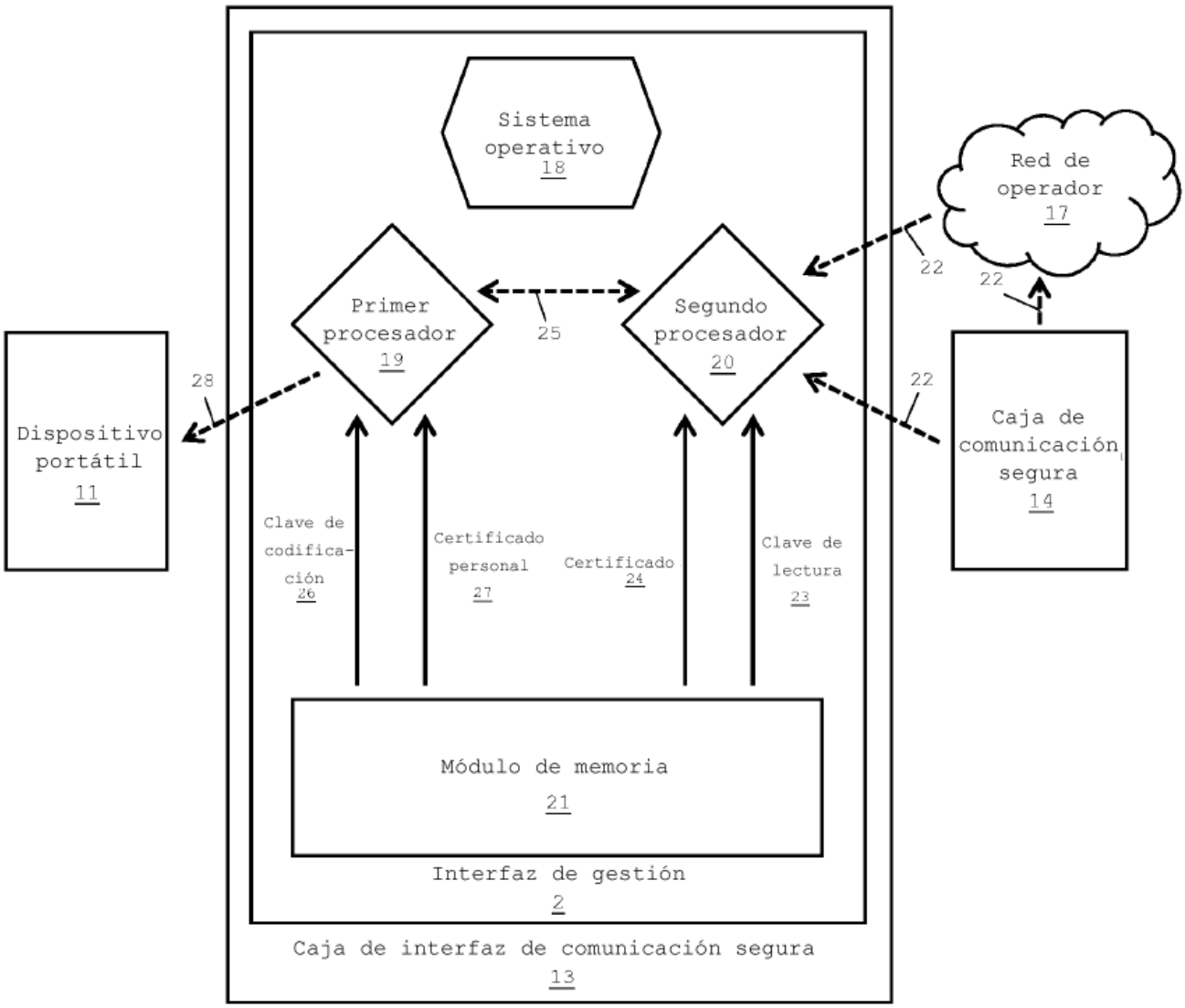
Sistema operativo 18
Red de operador 17
Primer procesador 19
25
Segundo procesador 20
22
22
22
28
Dispositivo portátil 11
Caja de comunicación segura 14
Clave de codificación 26
Certificado personal 27
Certificado 24
Clave de lectura 23
Módulo de memoria 21
Interfaz de gestión 2
Caja de interfaz de comunicación segura 13

FIGURA 5

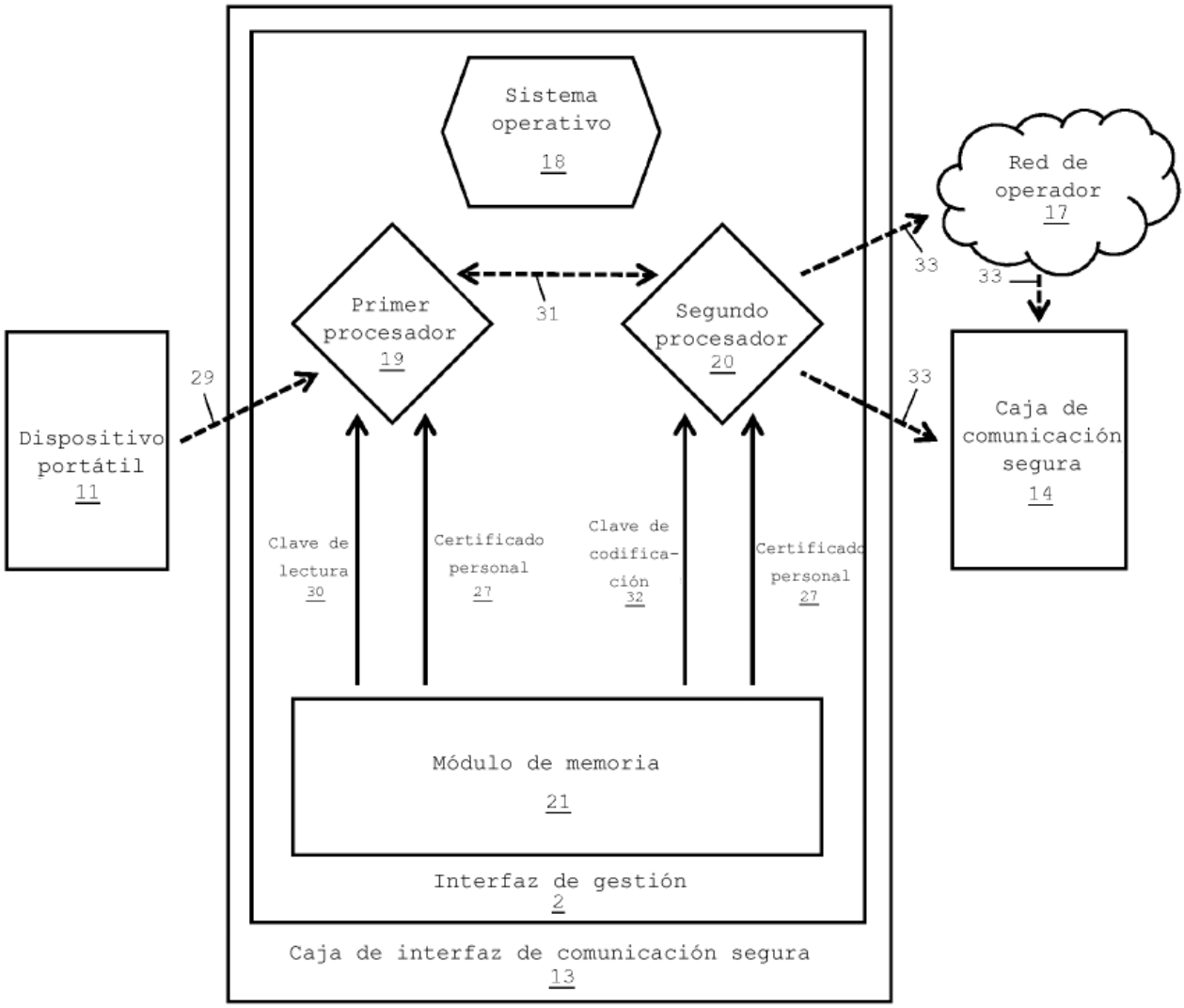
Sistema operativo
18
Red de operador
17
Primer procesador
19
31
Segundo procesador
20
33
33
33
29
Dispositivo portátil
11
Caja de comunicación segura
14
Clave de lectura
30
Certificado personal
27
Clave de codificación
32
Certificado personal
27
Módulo de memoria
21
Interfaz de gestión
2
Caja de interfaz de comunicación segura
13

FIGURA 6