(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 759 867**

(51) Int. CI.:

H04W 12/02 (2009.01)
H04L 29/06 (2006.01)
H04M 1/60 (2006.01)
H04L 9/06 (2006.01)
H04W 12/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **01.11.2011 PCT/FI2011/050961**

(87) Fecha y número de publicación internacional: **10.05.2013 WO13064717**

(96) Fecha de presentación y número de la solicitud europea: **01.11.2011 E 11875081 (9)**

(97) Fecha y número de publicación de la concesión europea: **11.09.2019 EP 2774400**

(54) Título: **Equipos de comunicación para comunicación segura**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.05.2020

(73) Titular/es:

SAVOX COMMUNICATIONS OY AB (LTD) (100.0%)
Keilaranta 15 B
02150 Espoo, FI

(72) Inventor/es:

AURANEN, PASI

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Equipos de comunicación para comunicación segura

Campo de la invención

La invención se refiere a equipos de comunicación que proporciona comunicación segura y comprende un dispositivo de interfaz de usuario y un dispositivo de comunicación que están interconectados a través de un enlace de datos. Además, la invención se refiere a un procedimiento con el fin de proporcionar una comunicación segura con el equipo de comunicación, al dispositivo de interfaz de usuario y a un programa informático con el fin de proporcionar una comunicación segura con el equipo de comunicación.

Antecedentes

En muchos casos hay una necesidad de equipos de comunicación cuya funcionalidad se distribuye a dos o más distintos dispositivos que están interconectados con un enlace de datos de corto alcance. Uno de los dispositivos del equipo de comunicación es a menudo un dispositivo de comunicación capaz de proporcionar conexiones a redes de comunicaciones externas y otro de los dispositivos es a menudo un dispositivo de interfaz de usuario que puede comprender, por ejemplo, un micrófono y un auricular y que está conectado al dispositivo de comunicación a través del enlace de datos de corto alcance. Por ejemplo, el equipo de comunicación puede ser un equipo de radio móvil donde el dispositivo de comunicación es un dispositivo de radio adecuado para conexiones de radio de largo alcance y el dispositivo de interfaz de usuario puede ser, por ejemplo, un auricular que está conectado de forma inalámbrica al dispositivo de radio a través de un enlace de radio de corto alcance. El equipo de comunicación del tipo descrito anteriormente se presenta, por ejemplo, en la publicación US2011034125.

Con el fin de proporcionar una comunicación segura, no es suficiente que sólo estén codificadas las conexiones de radio de largo alcance mencionadas anteriormente, pero se necesita el cifrado en el enlace de radio de corto alcance también. El enlace de radio de corto alcance puede ser, por ejemplo, pero no necesario, un enlace de radio Bluetooth®.

La publicación EP2106169 divulga un equipo de comunicación en el que el dispositivo de interfaz de usuario es un auricular y el dispositivo de comunicación es un dispositivo de radio adecuado para conexiones de radio de largo alcance. En las conexiones de radio de largo alcance, se emplea un algoritmo criptográfico en combinación con una clave para cifrar y descifrar información. El enlace de radio de corto alcance entre el auricular y el dispositivo de radio se asegura con la ayuda de una lista grabada de bits aleatorios que se copian tanto en el dispositivo de radio como en el auricular. Tanto en el dispositivo de radio como en el auricular, los bits aleatorios de la lista grabada se combinan en una compuerta OR exclusiva con datos digitales que transportan información de audio. Así, por ejemplo, la información transferida desde el auricular al dispositivo de radio se cifra en el auricular y se descifra en el dispositivo de radio. La lista de registradores de los bits aleatorios puede formarse, por ejemplo, alimentando el ruido producido de forma natural o artificial en el algoritmo criptográfico y almacenando los bits resultantes en una memoria.

En muchos casos, el dispositivo de interfaz de usuario comprende no sólo medios para convertir la voz en datos digitales y viceversa, sino también una interfaz de usuario para la recepción de comandos que controlan el funcionamiento de todo el equipo de comunicación. La interfaz de usuario puede comprender, por ejemplo, un botón de pulsar para hablar y/o un teclado. Para lograr una inmunidad suficiente a los ataques “DoS” de denegación de servicio, es importante que también los datos de eventos que representan los comandos recibidos a través de la interfaz de usuario estén cifrados adecuadamente. En los casos en que los datos del evento no se cifran correctamente, ciertos tipos de señales de interferencia pueden hacer que, por ejemplo, el dispositivo de comunicación crea que, por ejemplo, el botón pulsar para hablar del dispositivo de interfaz de usuario se presiona continuamente o que nunca se presiona. Esto naturalmente perturbaría o incluso impediría el funcionamiento del equipo de comunicación.

La solución obvia al problema descrito anteriormente es implementar el enlace de datos de corto alcance entre el dispositivo de interfaz de usuario y el dispositivo de comunicación con transceptores que soportan un algoritmo criptográfico adecuado con el fin de cifrar los datos enteros corriente transferidos en el corto enlace de datos de rango. Gehrmann C propone este enfoque, por ejemplo: “Bluetooth Security White Paper”, Bluetooth SIG Security Expert Group, 2002-04-19. Junto con muchos transceptores disponibles comercialmente, por ejemplo, transceptores Bluetooth® seguros, el inconveniente relacionado con este enfoque es que reemplazar el algoritmo criptográfico con otro algoritmo criptográfico requiere reemplazar el transceptor con otro transceptor. Por lo tanto, es difícil proporcionar tales dispositivos de interfaz de usuario, por ejemplo, micrófonos de altavoz remotos y dispositivos de comunicación que sean flexibles para admitir diferentes algoritmos criptográficos. Por lo tanto, es difícil lograr la interoperabilidad entre, por ejemplo, micrófonos de altavoz y dispositivos de radio remotos fabricados por diferentes proveedores.

Sumario

A continuación, se presenta un sumario simplificado con el fin de proporcionar una comprensión básica de algunos aspectos de las diversas realizaciones de la invención. El sumario no es una descripción general extensa de la invención. No se pretende identificar elementos clave o críticos de la invención ni delinear el alcance de la invención. El siguiente sumario simplemente presenta algunos conceptos de la invención en una forma simplificada como preludio de una descripción más detallada de realizaciones ejemplares de la invención.

De acuerdo con el primer aspecto de la invención, se proporciona un nuevo dispositivo de interfaz de usuario adecuada para ser una parte del equipo de comunicación cuya funcionalidad se distribuye a dispositivos separados interconectados con un enlace de datos. El dispositivo de interfaz de usuario de acuerdo con la invención comprende:

- una interfaz de usuario para recibir acciones de comando de un usuario,

- un procesador para a) recibir un primer flujo de datos digitales, b) generar datos de eventos digitales de acuerdo con las acciones de comando dirigidas a interfaz de usuario, c) para combinar los datos de eventos digitales con el primer flujo de datos digitales para formar un segundo flujo de datos digitales, y d) para cifrar el segundo flujo de datos digitales para formar un tercer flujo de datos digitales de acuerdo con la criptografía controlar los datos accesibles para el procesador, y

- un transmisor para transmitir el tercer flujo de datos digitales al enlace de datos.

El primer flujo de datos digital puede ser, por ejemplo, pero no necesariamente, los datos de salida digital de un codificador de audio. Como el cifrado se realiza después de combinar los datos del evento con el primer flujo de datos digitales, se cifran tanto los datos del evento como el primer flujo de datos digitales. Esto proporciona protección contra escuchas dirigidas al primer flujo de datos digitales que puede representar, por ejemplo, información de audio y contra ataques contra los datos de eventos que representan las acciones de comando del usuario. Por otro lado, el cifrado se realiza con el procesador antes de que el flujo de datos digitales se suministre al transmisor. Por lo tanto, no hay necesidad de utilizar un transmisor que esté dispuesto para soportar un algoritmo criptográfico. El procesador está dispuesto para cifrar el segundo flujo de datos digitales de acuerdo con los datos de control criptográfico que son accesibles al procesador. Por lo tanto, el dispositivo de interfaz de usuario se puede configurar para admitir diferentes algoritmos criptográficos al cargar los datos de control criptográfico apropiados que definen el algoritmo criptográfico y las claves necesarias para cifrar el segundo flujo de datos digitales. Los datos de control criptográfico pueden formar parte de una biblioteca de datos de control criptográfico, y el procesador puede disponerse para seleccionar una parte apropiada de la biblioteca con la ayuda de uno o más parámetros de control. En este caso, el dispositivo de interfaz de usuario se puede configurar fácilmente para admitir cualquiera de esos algoritmos criptográficos que se definen en la biblioteca.

De acuerdo con el segundo aspecto de la invención, se proporciona nuevo equipo de comunicación cuya funcionalidad es distribuida a un dispositivo de interfaz de usuario de acuerdo con la invención y con un dispositivo de comunicación que está interconectado con el dispositivo de interfaz de usuario a través de un enlace de datos. El dispositivo de comunicación del equipo de comunicación comprende:

- un receptor para recibir el tercer flujo de datos digitales desde el enlace de datos,

- un procesador para a) descifrar el tercer flujo de datos digitales para regenerar el segundo flujo de datos digitales y para b) separar los datos de eventos digitales y el primer flujo de datos digitales del segundo flujo de datos digitales regenerado, y

- un transmisor para transmitir información transportada por el primer flujo de datos digitales a una red de comunicaciones,

en el que el procesador del dispositivo de comunicación está dispuesto para controlar la operación del transmisor de acuerdo con los datos de eventos digitales.

De acuerdo con el tercer aspecto de la invención, se proporciona un nuevo procedimiento para proporcionar una comunicación segura entre un dispositivo de interfaz de usuario del equipo de comunicación y un dispositivo de comunicación del equipo de comunicación. El procedimiento de acuerdo con la invención comprende las siguientes acciones en el dispositivo de interfaz de usuario:

- utilizar un procesador para recibir un primer flujo de datos digitales cuya información debe transmitirse al dispositivo de comunicación,

- utilizar el procesador para generar datos de eventos digitales de acuerdo con las acciones de comando dirigidas a una interfaz de usuario,

- utilizar el procesador para combinar los datos de eventos digitales con el primer flujo de datos digitales para formar un segundo flujo de datos digitales,

- utilizar el procesador para cifrar el segundo flujo de datos digitales para formar un tercer flujo de datos digitales de acuerdo con los datos de control criptográfico accesibles al procesador, y

- entregar el tercer flujo de datos digitales a un transmisor del dispositivo de interfaz de usuario para transmitir el tercer flujo de datos digitales al dispositivo de comunicación a través de un enlace de datos.

De acuerdo con el cuarto aspecto de la invención, se proporciona un nuevo programa de ordenador para proporcionar una comunicación segura entre un dispositivo de interfaz de usuario del equipo de comunicación y un dispositivo de comunicación del equipo de comunicación. El programa de ordenador comprende instrucciones ejecutables por ordenador para controlar un procesador programable del dispositivo de interfaz de usuario para:

- generar datos de eventos digitales de acuerdo con acciones de comando dirigidas a una interfaz de usuario,

- combinar los datos de eventos digitales con un primer flujo de datos digitales para formar un segundo flujo de datos digitales,

- cifrar el segundo flujo de datos digitales para formar un tercer flujo de datos digitales de acuerdo con los datos de control criptográfico accesibles al procesador programable, y

- controlar un transmisor del dispositivo de interfaz de usuario para transmitir el tercer flujo de datos digitales al enlace de datos.

Un producto de programa de ordenador de acuerdo con la invención comprende un medio legible por ordenador, por ejemplo, un disco compacto, codificado con las instrucciones ejecutables por ordenador mencionado anteriormente.

A partir de la siguiente descripción de las realizaciones a modo de ejemplo, cuando se lean en relación con los dibujos adjuntos, se comprenderán mejor varias formas de realización ejemplificativas de la invención, tanto en cuanto a construcciones como a procedimientos de operación, junto con objetos adicionales y ventajas de las mismas.

Las realizaciones ejemplares de la invención se presentan en este documento no se han de interpretar para plantear limitaciones a la aplicabilidad de las reivindicaciones adjuntas. El verbo “comprender” se usa en este documento como una limitación abierta que no excluye ni requiere la existencia de características no mencionadas. Las características enumeradas en las reivindicaciones dependientes se pueden combinar mutuamente libremente, a menos que se indique lo contrario explícitamente.

Breve descripción de las figuras

Las realizaciones de la invención presentada en el sentido de ejemplos y sus ventajas se explican en mayor detalle a continuación con referencia a los dibujos que se acompañan, en los que

la figura 1 muestra un diagrama de bloques funcional de los equipos de comunicación de acuerdo con una realización de la invención,

las figuras 2a y 2b muestran equipos de comunicación de acuerdo con realizaciones de la invención, y

la figura 3 es un diagrama de flujo de un procedimiento de acuerdo con una realización de la invención para proporcionar comunicación segura entre un dispositivo de interfaz de usuario de equipo de comunicación y un dispositivo de comunicación del equipo de comunicación.

Descripción de las realizaciones ejemplificativas

La figura 1 muestra un diagrama de bloques funcional del equipo de comunicación de acuerdo con una realización de la invención. El equipo de comunicación comprende un dispositivo 101 de interfaz de usuario y un dispositivo 112 de comunicación que están interconectados con un enlace de radio de corto alcance. El equipo de comunicación puede ser, por ejemplo, un equipo de radio móvil donde el dispositivo 112 de comunicación es un dispositivo de radio adecuado para proporcionar conexiones de radio de larga duración y el dispositivo 101 de interfaz de usuario puede ser, por ejemplo, un micrófono-altavoz remoto “RSM”.

El dispositivo 101 de interfaz de usuario comprende una interfaz 102 de usuario para recibir acciones de comando de un usuario del equipo de comunicación. La interfaz de usuario puede comprender, por ejemplo, un botón 111 de pulsar para hablar y/o un teclado. El dispositivo 101 de interfaz de usuario comprende un procesador 104 dispuesto para recibir un primer flujo 131 de datos digitales que representa una señal de salida digital de un codificador 107 de audio. El codificador 107 de audio produce el primer flujo de datos digitales al convertir, en una forma digital, una primera señal analógica que representa una señal de salida analógica de un micrófono 109. El procesador 104 está dispuesto preferiblemente para llevar a cabo ciertas acciones de preprocesamiento dirigidas al primer flujo de datos digitales. Estas acciones de preprocesamiento pueden comprender, por ejemplo, codificar el primer flujo de datos digitales en un formato de compresión deseado y empaquetar el primer flujo de datos digitales para un tamaño de bloque adecuado para operaciones adicionales. En la figura 1, un bloque 118 funcional que preferiblemente está implementado por software, representa las acciones de preprocesamiento. El procesador 104 está dispuesto para generar datos de eventos digitales de acuerdo con las acciones de comando dirigidas a la interfaz 102 de usuario. Los datos de eventos digitales pueden indicar, por ejemplo, si se está presionando o no el botón 111 de pulsar para hablar. Además, los datos de eventos digitales pueden indicar pulsaciones de teclas dirigidas al teclado de la interfaz de usuario.

El procesador 104 está dispuesto para combinar los datos de eventos digitales con los primeros flujos de datos digitales con el fin de formar la corriente de unos segundos datos 132 digitales que contienen tanto el primer flujo de datos digitales como los datos de eventos digitales. El segundo flujo de datos digitales puede ser, por ejemplo, un flujo de paquetes de datos, de modo que la carga útil de cada paquete de datos contenga parte del primer flujo de datos digitales y el encabezado o tráiler de cada paquete de datos contenga parte de los datos del evento. Por ejemplo, el encabezado de cada paquete de datos del segundo flujo 132 de datos digitales puede expresar el estado del botón 111 de pulsar para hablar y/o las pulsaciones de teclas más recientes dirigidas al teclado, y la carga útil de cada paquete de datos puede contener información digitalizada de audio, video o audio-video. En la figura 1, un bloque 122 funcional que preferiblemente está implementado por software, representa una aplicación para combinar los datos de eventos digitales con el primer flujo de datos digitales y para controlar el enrutamiento de datos digitales entre diferentes bloques funcionales implementados con el procesador 104.

El procesador 104 está dispuesto para cifrar el segundo flujo de datos digitales para formar un tercer flujo de datos 133 digitales de acuerdo con los datos de control criptográfico accesibles al procesador. Los datos de control criptográfico pueden comprender uno o más conjuntos de instrucciones ejecutables del procesador, es decir, uno o más códigos de programa, que definen uno o más algoritmos criptográficos. Además, los datos de control criptográfico pueden comprender los parámetros de configuración requeridos, por ejemplo, claves de cifrado/descifrado, de uno o más algoritmos criptográficos. El uno o más algoritmos criptográficos pueden ser, por ejemplo, DES (Estándar de cifrado de datos), AES (Estándar de cifrado avanzado), IDEA (Algoritmo internacional de cifrado de datos), Blowfish, Twofish y/o triple DES. En la figura 1, un bloque 119 funcional que preferiblemente está implementado por software, representa la funcionalidad criptográfica. El dispositivo 101 de interfaz de usuario puede configurarse para admitir diferentes algoritmos criptográficos cargando datos de control criptográfico apropiados que definen el algoritmo criptográfico y los parámetros criptográficos apropiados. Como se indicó anteriormente, es posible que los datos de control criptográfico contengan datos relacionados con muchos algoritmos criptográficos diferentes. En este caso, el procesador 104 puede estar dispuesto para seleccionar un algoritmo criptográfico deseado en base a uno o más parámetros de control. El dispositivo 101 de interfaz de usuario puede comprender un elemento 120 de memoria para almacenar los datos de control criptográfico. También es posible que el procesador 104 contenga tanta memoria interna que los datos de control criptográfico puedan almacenarse en el procesador.

El procesador 104 está dispuesto para entregar el flujo de datos digitales cifrados a un transmisor 105 del dispositivo 101 de interfaz de usuario. Dependiendo del protocolo de transmisión utilizado en el enlace de radio de corto alcance entre el dispositivo de interfaz de usuario y el dispositivo 112 de comunicación, el procesador 104 puede estar dispuesto para procesar el flujo de datos digitales a transmitir con acciones relacionadas con el protocolo de transmisión. En la figura 1, un bloque 121 funcional que preferiblemente está implementado por software, representa las acciones relacionadas con el protocolo de transmisión. Las acciones relacionadas con el protocolo de transmisión pueden ser, por ejemplo, acciones relacionadas con una pila de protocolos de radio de corto alcance.

El dispositivo 112 de comunicación de los equipos de comunicación comprende un primer receptor 113 para recibir el tercer flujo de datos digitales desde el dispositivo 101 de interfaz de usuario a través del enlace de radio de corto alcance. El dispositivo 112 de comunicación comprende un procesador 114 dispuesto para descifrar el tercer flujo de datos digitales para regenerar el segundo flujo de datos digitales y para separar los datos de eventos digitales y el primer flujo de datos digitales del segundo flujo de datos digitales regenerado. El dispositivo 112 de comunicación comprende un primer transmisor 115 para transmitir información transportada por el primer flujo de datos digitales a una red 123 de comunicaciones que puede ser, por ejemplo, una red de radio celular y que se presenta como una nube sombreada en la figura 1. El procesador 114 es dispuesto para controlar el funcionamiento del transmisor 115 del dispositivo de comunicación de acuerdo con los datos de eventos digitales. Por ejemplo, el procesador 114 puede estar dispuesto para activar o desactivar el transmisor 115 de acuerdo con el estado del botón 111 de pulsar para hablar expresado por los datos del evento, y/o para determinar el nivel de potencia de transmisión, el código de línea, el código de canal y/u otros factores relacionados con la transmisión en función de los datos del evento.

En el equipo de comunicación de acuerdo con una realización de la invención, el dispositivo 112 de comunicación comprende un segundo receptor 117 para la recepción de información digital de la red 123 de comunicaciones. El procesador 114 del dispositivo de comunicación está dispuesto para cifrar la información digital recibida de la red de comunicaciones de acuerdo con los datos de control criptográfico accesibles al procesador 114 para formar un cuarto flujo de datos digitales. Los datos de control criptográfico son los mismos que se usan en el dispositivo 101 de interfaz de usuario y pueden almacenarse en un elemento 124 de memoria o en el procesador 114. El dispositivo de comunicación comprende un segundo transmisor 116 para transmitir el cuarto flujo de datos digitales al dispositivo 101 de interfaz de usuario a través del enlace de radio de corto alcance. El dispositivo 101 de interfaz de usuario comprende un receptor 106 para recibir el cuarto flujo 134 de datos digitales desde el dispositivo 112 de comunicación a través del enlace de datos de radio de corto alcance. El procesador 104 del dispositivo de interfaz de usuario está dispuesto para descifrar el cuarto flujo de datos digitales de acuerdo con los datos de control criptográfico accesibles al procesador 104 a fin de formar un quinto flujo 135 de datos digitales y emitir el quinto flujo de datos digitales. El dispositivo 101 de interfaz de usuario comprende un decodificador 108 de audio conectado al procesador 104 y dispuesto para convertir el quinto flujo de datos digitales en una segunda señal analógica. El dispositivo de interfaz de usuario comprende además un elemento 110 de altavoz o un auricular para convertir la segunda señal analógica en voz. El equipo de comunicación de acuerdo con esta realización de la invención es capaz de proporcionar comunicación bidireccional. En una realización a modo de ejemplo de la invención, el transmisor 115 y el receptor 117

del dispositivo 112 de comunicación están dispuestos para proporcionar funcionalidades de señalización para permitir conexiones marcadas a una red telefónica pública conmutada “PSTN” para que la marcación se realice de acuerdo con los datos del evento digital recibida desde el dispositivo 101 de interfaz de usuario.

El transmisor 105 y el receptor 106 del dispositivo 101 de terminal de usuario, y, correspondientemente, el transmisor 116 y el receptor 113 del dispositivo 112 de comunicación puede ser, por ejemplo, dispuesto para proporcionar el enlace de radio de corto alcance en una o más bandas de radio “ISM” Industriales, Científicas y Médicas definidas por las especificaciones 5.138, 5.150 y 5.280 del UIT-R del Reglamento de Radiocomunicaciones. El enlace de radio de corto alcance puede ser, por ejemplo, un enlace de radio Bluetooth® que funciona a una frecuencia central de 2,45 GHz, un enlace de radio de radio de alto rendimiento “HiperLAN” que funciona a una frecuencia central de 5,8 GHz, un enlace de radio IEEE 802.11/WiFi que funciona a Frecuencia central de 2,45 o 5,8 GHz, o IEEE 802.15.4, enlace de radio ZigBee que funciona a una frecuencia central de 915 MHz o 2,45 GHz.

En el caso del ejemplo mostrado en la figura 1, el dispositivo 101 de interfaz de usuario comprende el micrófono 109 para la conversión de voz en una señal analógica, el codificador 107 de audio para convertir la señal analógica a los flujos 131 de datos digitales, el decodificador 108 de audio para convertir el flujo 135 de datos digitales en una señal analógica y un elemento 110 de altavoz para convertir la señal analógica en voz. Sin embargo, debe tenerse en cuenta que el dispositivo 101 de interfaz de usuario también podría comprender conectores apropiados para recibir, por ejemplo, un módulo enchufable que comprende un micrófono, un elemento de altavoz o un auricular y un códec de audio. Además, debe observarse que en algunas aplicaciones el enlace de datos entre el dispositivo 101 de interfaz de usuario y el dispositivo 112 de comunicación podría ser, por ejemplo, un enlace de datos infrarrojo en lugar de un enlace de radio de corto alcance. El procesador 104 del dispositivo 101 de interfaz de usuario puede comprender uno o más circuitos de procesador. En consecuencia, el procesador 114 del dispositivo 112 de comunicación puede ser un solo circuito de procesador o puede comprender muchos circuitos de procesador. Cada circuito de procesador puede ser un circuito de procesador programable, un circuito eléctrico dedicado como, por ejemplo, un Circuito Integrado de Aplicación Específica “ASIC”, un circuito eléctrico configurable como, por ejemplo, una matriz de puerta programable de campo “FPGA”, o una combinación de dos o más de las alternativas mencionadas anteriormente.

Las figuras 2a y 2b muestran equipos de comunicación de acuerdo con realizaciones de la invención. El equipo de comunicación que se muestra en la figura 2a comprende un dispositivo 201 de interfaz de usuario que es un micrófono de altavoz remoto equipado con un botón 211 de pulsar para hablar. El equipo de comunicación comprende un dispositivo 212 de comunicación que puede transportarse, por ejemplo, en una correa 250 de un usuario y que proporciona conexiones a una red de comunicaciones externa de acuerdo con el estado del botón 211 de pulsar para hablar. El dispositivo 212 de comunicación y el dispositivo 201 de interfaz de usuario comprenden transceptores de radio de corto alcance para proporcionar un enlace de radio bidireccional de corto alcance entre el dispositivo 212 de comunicación y el dispositivo 201 de interfaz de usuario. El equipo de comunicación que se muestra en la figura 2a puede ser, por ejemplo, tal como se explica con la ayuda de la figura 1. El equipo de comunicación que se muestra en la figura 2b comprende un dispositivo 201a de interfaz de usuario que es una unidad de cámara remota equipada con un teclado. El equipo de comunicación comprende un dispositivo 212a de comunicación que proporciona conexiones a una red de comunicaciones externa de acuerdo con las pulsaciones de teclas dirigidas al teclado. El dispositivo 201a de interfaz de usuario comprende un transmisor de radio de corto alcance y el dispositivo 212a de comunicación comprende un receptor de radio de corto alcance para proporcionar un enlace de radio unidireccional de corto alcance desde el dispositivo 201a de interfaz de usuario al dispositivo 212a de comunicación. Como se indica en el ejemplo mostrado en la figura 2b, la aplicabilidad de la presente invención no se limita a casos en los que hay una comunicación bidireccional o transferencia de datos entre el dispositivo de interfaz de usuario y el dispositivo de comunicación del equipo de comunicación.

La figura 3 es un diagrama de flujo de un procedimiento de acuerdo con una realización de la invención para proporcionar comunicación segura entre un dispositivo de interfaz de usuario de equipo de comunicación y un dispositivo de comunicación del equipo de comunicación. El procedimiento comprende las siguientes acciones en el dispositivo de interfaz de usuario:

- acción 301: recibir un primer flujo de datos digitales cuya información debe transmitirse desde el dispositivo de interfaz de usuario al dispositivo de comunicación,

- acción 302: generar datos de eventos digitales en de acuerdo con las acciones de comando dirigidas a una interfaz de usuario,

- acción 303: combinar los datos de eventos digitales con el primer flujo de datos digitales para formar un segundo flujo de datos digitales,

- acción 304: utilizar un procesador para cifrar el segundo flujo de datos digitales para formar un tercer flujo de datos digitales de acuerdo con los datos de control criptográfico que son accesibles al procesador, y

- acción 305: entregar el tercer flujo de datos digitales a un transmisor del dispositivo de interfaz de usuario para transmitir el tercer flujo de datos digitales al dispositivo de comunicación a través de un enlace de datos.

Un procedimiento de acuerdo con una realización de la invención comprende además las siguientes acciones en el dispositivo de comunicación del equipo de comunicación:

- recibir el tercer flujo de datos digitales desde el enlace de datos,

- utilizar un procesador del dispositivo de comunicación para descifrar el tercer flujo de datos digitales para regenerar el segundo flujo de datos digitales de acuerdo con los datos de control criptográfico que se han hecho accesibles también al procesador del dispositivo de comunicación,

- separar los datos de eventos digitales y el primer flujo de datos digitales del segundo flujo de datos digitales regenerados,

- transmitir información transportada por el primer flujo de datos digitales a una red de comunicaciones, y

- controlar, de acuerdo con los datos de eventos digitales, la transmisión de la información transportada por el primer flujo de datos digitales.

Un procedimiento de acuerdo con una realización de la invención comprende además las siguientes acciones a fin de permitir la comunicación bidireccional:

- recibir, en el dispositivo de comunicación, la información digital de la red de comunicaciones,

- utilizar un procesador del dispositivo de comunicación para el cifrado de la información digital recibida de la red de comunicaciones para formar un cuarto flujo de datos digitales de acuerdo con los datos de control criptográfico accesibles al procesador del dispositivo de comunicación,

- entregar el cuarto flujo de datos digitales a un transmisor de corto alcance del dispositivo de comunicación para transmitir el cuarto flujo de datos digitales al dispositivo de interfaz de usuario a través del enlace de datos,

- recibir, en el dispositivo de interfaz de usuario, el cuarto flujo de datos digitales,

- utilizar un procesador del dispositivo de interfaz de usuario para descifrar el cuarto flujo de datos digitales de acuerdo con Los datos de control criptográfico.

Un programa de ordenador de acuerdo con una realización de la invención comprende módulos de software para proporcionar una comunicación segura entre un dispositivo de interfaz de usuario del equipo de comunicación y un dispositivo de comunicación del equipo de comunicación. Los módulos de software comprenden instrucciones ejecutables por ordenador para controlar un procesador programable del dispositivo de interfaz de usuario para:

- generar datos de eventos digitales de acuerdo con acciones de comando dirigidas a una interfaz de usuario,

- combinar los datos de eventos digitales con un primer flujo de datos digitales para formar un segundo flujo de datos digitales,

- cifrar el segundo flujo de datos digitales para formar un tercer flujo de datos digitales de acuerdo con los datos de control criptográfico accesibles al procesador programable, y

- controlar un transmisor del dispositivo de interfaz de usuario para transmitir el tercer flujo de datos digital al enlace de datos.

En un programa de ordenador de acuerdo con una realización de la invención, los módulos de software adicionales de ordenador comprenden instrucciones ejecutables para el control de un procesador programable del dispositivo de comunicación para:

- descifrar los terceros flujos de datos digitales recibidos de los enlaces de datos para regenerar el segundo flujo de datos digitales,

- separar los datos de eventos digitales y el primer flujo de datos digital del segundo flujo de datos digitales regenerado,

- controlar un transmisor para transmitir la información transportada por el primer flujo de datos digitales a una red de comunicaciones, y

- controlar, de acuerdo con los datos de eventos digitales, la transmisión de la información transportada por el primer flujo de datos digitales.

Los módulos de software pueden ser, por ejemplo, subrutinas y funciones generadas con un lenguaje de programación adecuado.

Un producto de programa de ordenador de acuerdo con una realización de la invención comprende un medio legible por ordenador no volátil, por ejemplo, un disco compacto (“CD”), codificado con un programa de ordenador de acuerdo con una realización de la invención.

Una señal de acuerdo con una realización de la invención se codifica a la información de transporte que define un programa de ordenador de acuerdo con una realización de la invención.

Los ejemplos específicos proporcionados en la descripción dada anteriormente no se deben interpretar como limitantes. Por lo tanto, la invención no se limita simplemente a las realizaciones descritas anteriormente.

REIVINDICACIONES

1. Un dispositivo (101, 201, 201a) de interfaz de usuario que comprende:

- una interfaz (102) de usuario para recibir acciones de comando de un usuario,

- un procesador (104) para recibir un primer flujo de datos digitales, para generar datos de eventos digitales de acuerdo con las acciones de comando dirigidas a la interfaz de usuario, y para combinar los datos de eventos digitales con el primer flujo de datos digitales para formar un segundo flujo de datos digitales, y

- un transmisor (105) para transmitir un tercer flujo de datos digitales a un enlace de datos,

caracterizado porque el procesador está dispuesto para cifrar el segundo flujo de datos digitales para formar el tercer flujo de datos digitales de acuerdo con los datos de control criptográfico accesibles al procesador y para entregar el tercer flujo de datos digitales al transmisor (105)

2. Un dispositivo de interfaz de usuario de acuerdo con la reivindicación 1, en el que el dispositivo de interfaz de usuario comprende un receptor (106) para recibir un cuarto flujo de datos digitales desde el enlace de datos, y el procesador está dispuesto para descifrar el cuarto flujo de datos digitales para formar un quinto flujo de datos digitales y para generar el quinto flujo de datos digitales.

3. Un dispositivo de interfaz de usuario de acuerdo con la reivindicación 1, en el que el transmisor es un transmisor de radio configurado para operar a 2,45 GHz o 5,8 GHz o 915 MHz de frecuencia central.

4. Un dispositivo de interfaz de usuario de acuerdo con la reivindicación 1, en el que el dispositivo de interfaz de usuario comprende además un codificador (107) de audio conectado al procesador y dispuesto para convertir una primera señal analógica que transporta información de audio al primer flujo de datos digital.

5. Dispositivo de interfaz de usuario de acuerdo con la reivindicación 2, en el que el dispositivo de interfaz de usuario comprende además un decodificador (108) de audio conectado al procesador y dispuesto para convertir el quinto flujo de datos digitales en una segunda señal analógica.

6. Un dispositivo de interfaz de usuario de acuerdo con la reivindicación 1, en el que la interfaz de usuario comprende un botón (111) de pulsar para hablar y el procesador está dispuesto para configurar los datos de eventos digitales para indicar si se está presionando o no el botón de pulsar.

7. Un dispositivo de interfaz de usuario de acuerdo con la reivindicación 1, en el que la interfaz de usuario comprende un teclado y el procesador está dispuesto para configurar los datos de eventos digitales para indicar las pulsaciones de teclas dirigidas al teclado.

8. Equipo de comunicación que comprende un dispositivo (101, 201, 201a) de interfaz de usuario de acuerdo con cualquiera de las reivindicaciones 1-7 y un dispositivo (112, 212, 212a) de comunicación que comprende:

- un primer receptor (113) para recibir, a través de los enlaces de datos, el tercer flujo de datos digitales desde el dispositivo de interfaz de usuario,

- un procesador (114) para a) descifrar el tercer flujo de datos digitales para regenerar el segundo flujo de datos digitales y para b) separar los datos de eventos digitales y el primer flujo de datos digital del segundo flujo de datos digital regenerado, y

- un primer transmisor (115) para transmitir información transportada por el primer flujo de datos digitales a una red de comunicaciones,

en el que el procesador del dispositivo de comunicación está dispuesto para controlar el funcionamiento del transmisor del dispositivo de comunicación de acuerdo con los datos de eventos digitales.

9. Equipo de comunicación de acuerdo con la reivindicación 8, en el que el dispositivo de comunicación comprende además un segundo transmisor (116) para transmitir un cuarto flujo de datos digitales al dispositivo de interfaz de usuario a través del enlace de datos y un segundo receptor (117) para recibir información digital del red de comunicaciones, y el procesador del dispositivo de comunicación está dispuesto para cifrar la información digital recibida de la red de comunicaciones para formar el cuarto flujo de datos digitales.

10. Equipo de comunicación de acuerdo con la reivindicación 9, en el que el primer transmisor y el segundo receptor del dispositivo de comunicación están dispuestos para proporcionar conexiones marcadas con una red telefónica pública conmutada (PSTN) de acuerdo con los datos de eventos digitales.

11. Equipo de comunicación de acuerdo con la reivindicación 9, en el que el primer transmisor y el segundo receptor del dispositivo de comunicación están dispuestos para proporcionar conexiones con una red móvil celular.

12. Un procedimiento para proporcionar comunicación segura entre un dispositivo de interfaz de usuario del equipo de comunicación y un dispositivo de comunicación del equipo de comunicación, el procedimiento comprende las siguientes acciones en el dispositivo de interfaz de usuario:

- utilizar un procesador para recibir (301) un primer flujo de datos digital por el cual la se transmitirá información transportada al dispositivo de comunicación,

- utilizar el procesador para generar (302) datos de eventos digitales de acuerdo con las acciones de comando dirigidas a una interfaz de usuario,

- utilizar el procesador para combinar (303) los datos de evento digital con el primer flujo de datos digitales para formar un segundo flujo de datos digitales y

- entregar (305) un tercer flujo de datos digitales a un transmisor del dispositivo de interfaz de usuario para transmitir el tercer flujo de datos digitales al dispositivo de comunicación a través de un enlace de datos,

caracterizado porque el procedimiento comprende utilizar (304) el procesador para cifrar el segundo flujo de datos digitales para formar el tercer flujo de datos digital de acuerdo con los datos de control criptográfico accesibles al procesador.

13. Un procedimiento de acuerdo con la reivindicación 12, en el que el procedimiento comprende además las siguientes acciones en el dispositivo de comunicación del equipo de comunicación:

- recibir el tercer flujo de datos digitales desde el enlace de datos,

- descifrar el tercer flujo de datos digitales para regenerar el segundo flujo de datos digitales,

- separar los datos de eventos digitales y el primer flujo de datos digitales del segundo flujo de datos digitales regenerados,

- transmitir información transportada por el primer flujo de datos digitales a una red de comunicaciones, y

- controlar, de acuerdo con el evento digital datos, la transmisión de la información transportada por el primer flujo de datos digitales.

14. Un programa de ordenador que comprende instrucciones ejecutables por ordenador para controlar un procesador programable de un dispositivo de interfaz de usuario de equipo de comunicación para:

- generar datos de eventos digitales de acuerdo con acciones de comando dirigidas a una interfaz de usuario,

- combinar los datos de eventos digitales con un primer flujo de datos digital para formar un segundo flujo de datos digitales, y

- controlar un transmisor del dispositivo de interfaz de usuario para transmitir un tercer flujo de datos digitales a un enlace de datos,

caracterizado porque el programa informático comprende además instrucciones ejecutables por ordenador para controlar el procesador programable del dispositivo de comunicación para cifrar el segundo flujo de datos digitales para formar el tercer flujo de datos digitales de acuerdo con los datos de control criptográfico accesibles al procesador programable y entregar el tercer flujo de datos digitales al transmisor.

15. Un programa informático de acuerdo con la reivindicación 14, en el que el programa informático comprende además instrucciones ejecutables por ordenador para controlar un procesador programable de un dispositivo de comunicación del equipo de comunicación para:

- descifrar el tercer flujo de datos digitales recibido del enlace de datos para regenerar el segundo flujo de datos digitales,

- separar los datos de eventos digitales y el primer flujo de datos digitales del segundo flujo de datos digitales regenerado,

- controlar un transmisor para transmitir la información transportada por el primer flujo de datos digitales a una red de comunicaciones, y

- controlar, en de acuerdo con los datos de eventos digitales, la transmisión de la información transportada por el primer flujo de datos digitales.

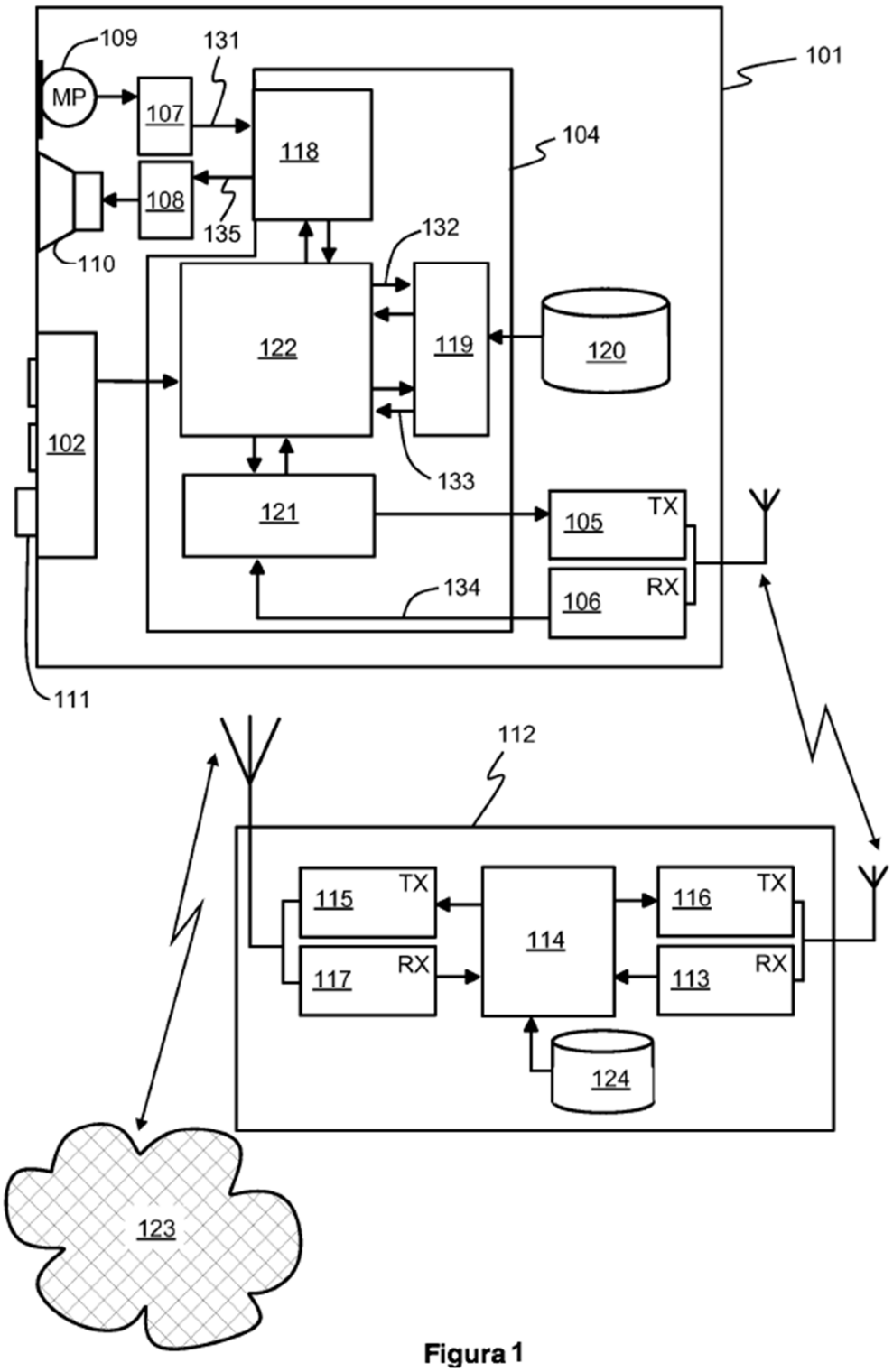
109
131
101
MP
107
118
104
108
135
132
110
122
119
120
102
133
121
105
TX
106
RX
134
111
112
115
TX
116
TX
114
117
RX
113
RX
124
123

Figura 1

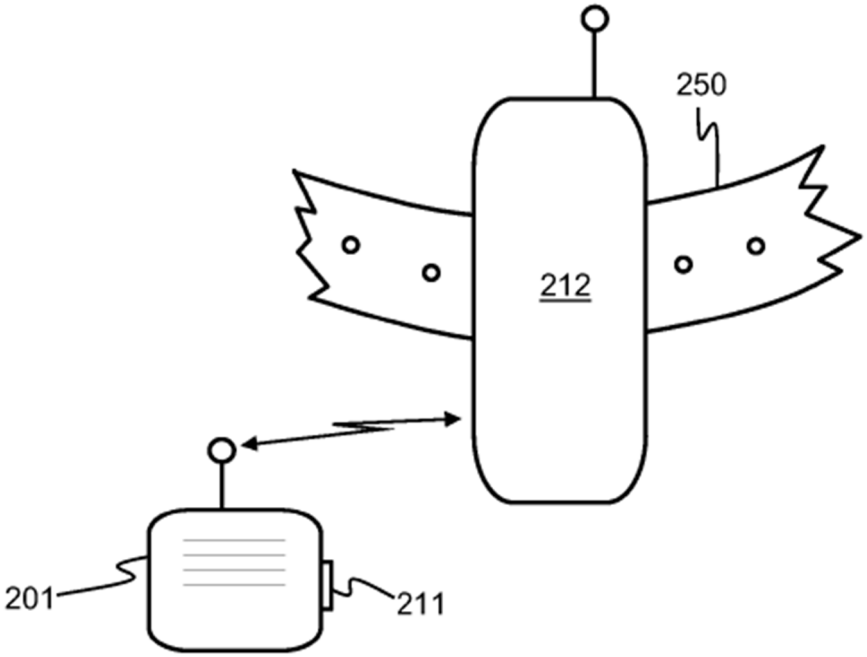

Figura 2a

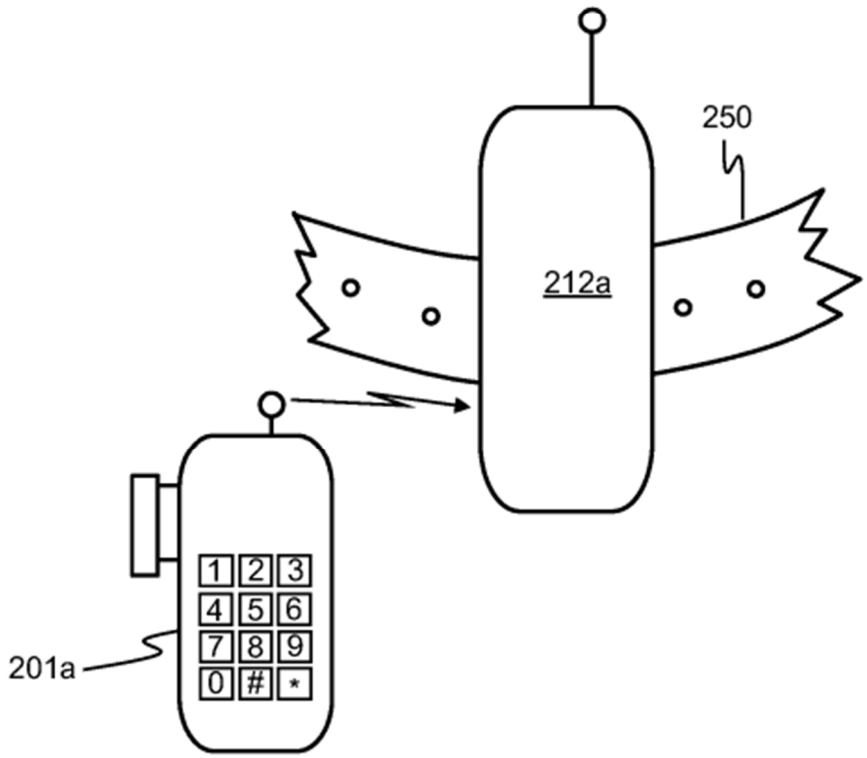

Figura 2b

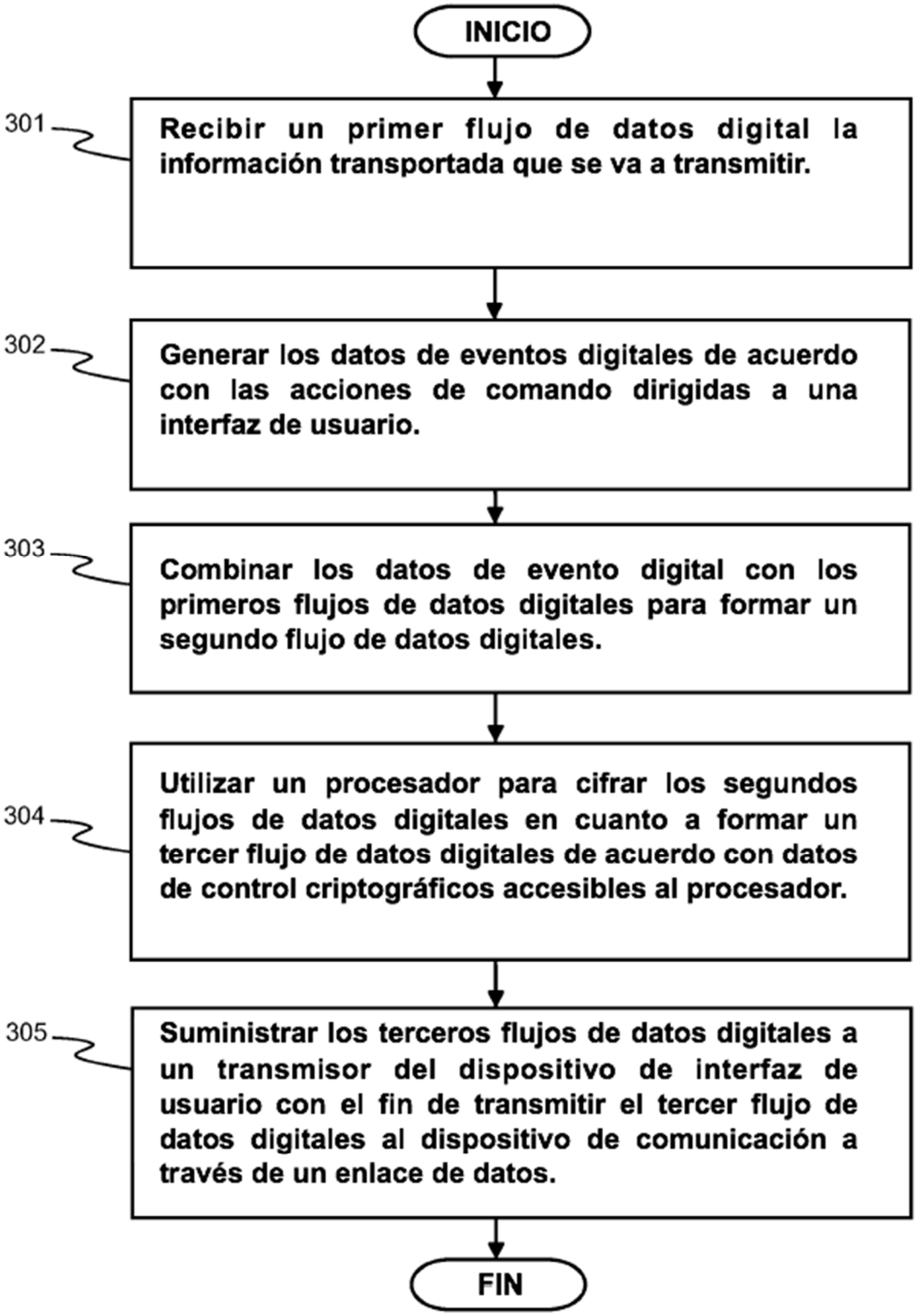
INICIO
301
Recibir un primer flujo de datos digital la información transportada que se va a transmitir.
302
Generar los datos de eventos digitales de acuerdo con las acciones de comando dirigidas a una interfaz de usuario.
303
Combinar los datos de evento digital con los primeros flujos de datos digitales para formar un segundo flujo de datos digitales.
304
Utilizar un procesador para cifrar los segundos flujos de datos digitales en cuanto a formar un tercer flujo de datos digitales de acuerdo con datos de control criptográficos accesibles al procesador.
305
Suministrar los terceros flujos de datos digitales a un transmisor del dispositivo de interfaz de usuario con el fin de transmitir el tercer flujo de datos digitales al dispositivo de comunicación a través de un enlace de datos.
FIN

Figura 3