(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 716 887**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/02 (2009.01)
G06F 21/86 (2013.01)
H04M 1/725 (2006.01)
H04W 4/00 (2008.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.09.2015 E 15184095 (6)**

(97) Fecha y número de publicación de la concesión europea: **16.01.2019 EP 3139564**

(54) Título: **Módulo de codificación de encriptado**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.06.2019

(73) Titular/es:

MARGENTO R&D D.O.O. (100.0%)
Gosposvetska cesta 84
2000 Maribor, SI

(72) Inventor/es:

CHOWDHURY, AMOR;
BLAZINSEK, IZTOK y
IGREC, DALIBOR

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

Observaciones :

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

DESCRIPCIÓN

Módulo de codificación de encriptado

Campo de la tecnología

Esta invención pertenece al campo de los dispositivos de codificación (encriptado) para propósitos de transferencia segura de voz (llamada telefónica), datos y mensajes. La invención está destinada a ser utilizada con teléfonos alámbricos o inalámbricos, teléfonos inteligentes, dispositivos inteligentes, tabletas, ordenadores personales o dispositivos similares (en lo sucesivo denominados: «dispositivo de comunicación»). La invención es un dispositivo que codifica (encripta) la voz (datos, mensajes) entre dos o más dispositivos conectados con el uso de conexión de voz o datos.

Problema técnico

El problema técnico abordado en la presente invención es el diseño de un dispositivo que permite que dos o más usuarios (dispositivos) tengan una conversación segura o una transferencia de datos, sin la posibilidad de interceptación (escucha) de voz (datos o mensaje) y decodificación (desencriptado) por una tercera parte (no autorizada). La conversación o la transferencia de datos se realiza con el uso de un dispositivo de comunicación.

El desarrollo de las telecomunicaciones en el último par de décadas hizo la escucha de llamadas telefónicas muy simple. Varias agencias de inteligencia y organizaciones privadas realizan la intercepción de llamada de rutina, lo que les permite adquirir información política, militar, económica y de otro tipo de manera ilegal. El equipo que permitía la intercepción de llamadas y mensajes de teléfonos móviles se convirtió en barato y fácilmente disponible, debido a lo cual las escuchas de llamadas se volvieron muy generalizadas, simples y sin control. Por lo tanto, el uso de un dispositivo propuesto con esta patente está perfectamente justificado, ya que el dispositivo garantiza la protección de la privacidad cuando se utiliza una conexión de voz o datos.

La protección de los datos de voz con una codificación fuerte y digna de confianza (encriptado) no es simple. La mayoría de los algoritmos de codificación (encriptación) utilizados en la actualidad son de dudosa calidad, ya que cada vez más estudios muestran que la mayoría de ellos incluyen varias formas relativamente simples de acceder a paquetes codificados (encriptados) o las llamadas "puertas traseras". Otra razón para desarrollar una mejor protección de la privacidad es el hecho de que los superordenadores modernos abusan de la débil protección de los algoritmos de codificación (encriptación) débiles. Los esfuerzos de marketing generalmente ocultan estas desventajas al público en general al garantizar que el problema rara vez se discute y se publica muy poco al respecto. Finalmente, las mismas agencias e instituciones que emiten certificados de idoneidad para tales algoritmos de codificación (encriptación) son los que en muchos casos son responsables de interceptar y escuchar los dispositivos de telecomunicaciones.

El documento US 2011/0222688 A1 se refiere a una solución de voz segura para un dispositivo móvil, en particular para un teléfono inteligente de tipo Blackberry™, en el que en un chip seguro se inserta en el dispositivo móvil y se utiliza para encriptar y desencriptar los paquetes de datos de voz para establecer conexiones seguras de extremo a extremo.

Sumario de la Invención

La solución propuesta según la reivindicación 1 permite una conversación, una transferencia de datos y una mensajería seguras entre usuarios finales o dispositivos de comunicación mediante el uso de un módulo de codificación de encriptado. El módulo de codificación de encriptado propuesto comprende los componentes básicos que se muestran en la figura 1:

- el módulo de codificación de encriptado con opción de fuente de alimentación autónoma (batería interna 112), unidad de fuente de alimentación 107, que incluye un sistema de administración de batería y tiene la opción de conectarse a la fuente de alimentación externa, su propia unidad de procesamiento 113, que puede, entre otras cosas, tener la forma de un microcontrolador, un circuito FPGA u otro elemento de procesamiento. El dispositivo está equipado con varios módulos de memoria 106, módulo sin contacto NFC 102, Bluetooth u otro tipo de módulo RF 103, conector de audio 104, toma de audio 108, micrófono para captura de sonido 110, altavoz principal III para reproducir sonido (voz), interfaz de USB 101, elemento de seguridad 105, que garantiza el almacenamiento seguro de los datos clave y también incluye un mecanismo para la detección y prevención del acceso no autorizado del módulo de codificación de encriptado y un altavoz secundario 109 para bloquear el micrófono incorporado en el dispositivo. La carcasa del módulo de codificación de encriptado está construida de tal manera que detecta la manipulación del interior del dispositivo y lo desactiva inmediatamente para su uso posterior (es a prueba de manipulación indebida, sensible a la manipulación indebida y resistente a la manipulación indebida, a prueba de manipulación indebida). Además, la carcasa puede deshabilitar el funcionamiento del micrófono primario del dispositivo de comunicación 100,

- una aplicación de software que se ejecuta en el dispositivo de comunicación para controlar el módulo de codificación de encriptado.

El diseño del módulo de codificación de encriptado se muestra en la figura 1. El módulo de codificación de encriptado puede estar dentro de la carcasa del dispositivo. La carcasa también sirve como barrera para deshabilitar la captura de sonido en el dispositivo de comunicación usado.

La electrónica interna del módulo de encriptado de codificación realiza las siguientes funciones básicas:

- captura de sonido,
- reproducción de sonido,
- codificación (encriptado) y decodificación (desencriptado) de sonido, datos y mensajes,
- comunicación con el uso de diferentes interfaces de comunicación.

El módulo de codificación de encriptado 205 puede establecer una conexión con el dispositivo de comunicación 204 (por ejemplo, teléfono móvil) de varias maneras (figura 2):

- interfaz USB 200,
- interfaz sin contacto NFC 201,
- interfaz Bluetooth 202 (también es posible utilizar otras interfaces inalámbricas, tal como banda RF ISM, ZigBee, WiFi, IR u otras),
- interfaz electroacústica (conjunto) 203.

Además de tener diferentes opciones para la conexión al dispositivo de comunicación, el módulo de codificación de encriptado puede establecer y mantener la comunicación en forma digital o analógica a través de todas las conexiones posibles disponibles para el dispositivo de comunicación (establecer y mantener un multiplex de comunicación) que hace que la interceptación de datos de forma simultánea más difícil o completamente imposible.

El módulo de codificación encriptado 300 puede estar conectado a dispositivos externos (por ejemplo, 303 y 304 y otros dispositivos externos) a través de las siguientes interfaces de comunicación (figura 3):

- interfaz Bluetooth 302 (por ejemplo, un auricular inalámbrico - 304, radio de coche - 305, también es posible utilizar otras interfaces inalámbricas, tal como banda de RF ISM, ZigBee, WiFi, IR u otras),
- interfaz de audio - 301 (por ejemplo, auriculares con cable - 303).

El módulo de codificación de encriptado puede funcionar en dos modos:

- como un dispositivo completamente autónomo (independiente), donde su presencia no se nota en el dispositivo de comunicación, y el dispositivo de comunicación no influye en su operación,
- en combinación con una aplicación en el dispositivo de comunicación. El procedimiento para comunicación segura:

  o el usuario inicia la aplicación en el dispositivo de comunicación 601,
  o él/ella se autentifica con un número PIN o un sensor biométrico 602; si la autentificación no es exitosa, el usuario debe autentificarse nuevamente,
  o si la autentificación es exitosa, el usuario ingresa el número o la dirección de la persona receptora o elige uno o más usuarios de los contactos 604,
  o el usuario comienza el procedimiento de establecer una conexión segura presionando un botón 605,
  o la aplicación informa al usuario sobre la conexión establecida entre los módulos de codificación de encriptado con éxito 606 o sin éxito 609,
  o transferencia de sonido/habla/datos/mensajes 607,
  o después de que se completa la conversación/transferencia de datos/intercambio de mensajes, el usuario finaliza la conexión 608.

La aplicación en el dispositivo de comunicación, que controla el módulo de codificación de encriptado, permite:

- control directo del módulo de codificación de encriptado (configuración, elección del tipo de interfaz de comunicación, etc.),
- establecimiento de una conexión segura,
- llamada segura,
- comunicación segura,
- transferencia segura de datos,
- mensajería segura,
- el acceso a la aplicación en el dispositivo de comunicación está restringido (PIN, verificación biométrica, etc.)
- gestión de los datos de otros usuarios de los módulos de codificación de encriptado, con los que se establece una conexión segura,

- actualización remota del firmware y configuración del módulo de codificación de encriptado.

Los módulos de codificación de encriptado establecen una conexión entre los mismos utilizando interfaces de comunicación del dispositivo de comunicación. El establecimiento de una conexión segura se realiza mediante el uso de dos interfaces de comunicación:

- conexión de datos (también es posible utilizar otras interfaces inalámbricas, tal como banda RF ISM, ZigBee, WiFi, etc.),
- conexión de voz (llamada).

La conexión entre los módulos de codificación de encriptado se puede establecer de dos formas:

- conexión directa, donde el módulo de codificación de encriptado 403 con el uso de una interfaz de comunicación en el dispositivo 402 establece una conexión segura 401 directamente al dispositivo 404, que envía los datos al módulo de codificación de encriptado 405 (figura 4),
- conexión indirecta, donde el módulo de codificación de encriptado 501 con el uso de una interfaz de comunicación en el dispositivo 502 establece primero una conexión segura 503 a un dispositivo interino 504. Este dispositivo luego inicia una nueva sesión segura 505 con el dispositivo final 506, y este último reenvía los datos recibidos al módulo de codificación de encriptado 507 (figura 5).

Los modos de operación del módulo de codificación de encriptado que se realizan si una conexión segura se establece con éxito entre los módulos de codificación de encriptado:

- transferencia de datos: los datos que deben transferirse se encuentran en el dispositivo de comunicación. El dispositivo de comunicación primero envía los datos al módulo de codificación de encriptado. El módulo de codificación de encriptado los codifica y los reenvía al dispositivo que los envía al dispositivo de comunicación del destinatario. Si se utiliza la conexión indirecta, los datos se envían primero al dispositivo interino que transmite los datos al dispositivo de comunicación del destinatario final. El dispositivo de comunicación del destinatario luego envía los datos a su módulo de codificación de encriptado, que los decodifica (desencripta) y envía el resultado al dispositivo de comunicación;
- mensajería: los mensajes que deben enviarse se encuentran en el dispositivo de comunicación. El dispositivo de comunicación transmite los mensajes al módulo de codificación de encriptado. El módulo de codificación de encriptado los codifica y los reenvía al dispositivo que los envía al dispositivo de comunicación del destinatario. Si se utiliza la conexión indirecta, los datos se envían primero al dispositivo interino que transmite los datos al dispositivo de comunicación del destinatario final. El dispositivo de comunicación del destinatario luego envía los mensajes a su módulo de codificación de encriptado, que los decodifica (desencripta) y envía el resultado al dispositivo de comunicación;
- establecimiento de una conexión de llamada (transferencia de sonido): La captura de sonido se realiza a través de un micrófono, que puede ubicarse en el módulo de codificación de encriptado, el dispositivo de comunicación o un dispositivo externo, conectado directamente al módulo de codificación de encriptado con una interfaz por cable o inalámbrica. Si el sonido se captura con el uso del dispositivo de comunicación, el sonido se envía primero al módulo de codificación de encriptado en forma de datos capturados; de lo contrario, los datos ya están en el módulo de codificación de encriptado ya que se capturan directamente con el micrófono interno o se reenvían desde el dispositivo externo. El módulo de codificación de encriptado los codifica y los reenvía al dispositivo de comunicación que los envía al dispositivo de comunicación del destinatario. Si se utiliza la conexión indirecta, los datos se envían primero al dispositivo interino que transmite los datos al dispositivo de comunicación del destinatario final. El dispositivo de comunicación del destinatario envía los datos recibidos a su módulo de codificación de encriptado, que los decodifica (desencripta) y los reproduce en la interfaz de comunicación elegida (el altavoz del dispositivo de comunicación, el altavoz del módulo de codificación de encriptado, reenviando a otros dispositivos externos).

Lista de abreviaciones

- NFC - Comunicación de campo cercano
- USB - Bus serie universal
- Bluetooth: tecnología de alta frecuencia inalámbrica segura para conectar diferentes dispositivos electrónicos digitales a pocos metros de distancia
- ZigBee: protocolo de comunicación inalámbrica destinado a redes personales con bajo consumo de energía.
- RF - radiofrecuencia
- WiFi - red inalámbrica
- FPGA - Matriz de puerta programable en campo
- Evidencia de manipulación - la capacidad de rastrear un acceso no autorizado
- Respuesta a la manipulación - la capacidad de responder ante cualquier acceso no autorizado
- Resistente a la manipulación: la capacidad de resistir cualquier acceso no autorizado
- A prueba de manipulaciones: la capacidad de imposibilitar el acceso no autorizado

REIVINDICACIONES

1. Un módulo de codificación de encriptado que permite la comunicación segura de llamadas/voz y datos para teléfonos con cable o inalámbricos, teléfonos inteligentes, dispositivos inteligentes, tabletas, ordenadores personales y dispositivos similares que están integrados o en comunicación/conexión con el módulo de codificación de encriptado, en el que se proporciona un alto nivel de la seguridad que es completamente independiente de los elementos de seguridad del dispositivo de comunicación, que comprende

- una batería interna (112),
- una unidad de fuente de alimentación que puede incluir una conexión externa para cargar la batería, en donde la fuente de alimentación incluye también las lógicas de control de la batería (107),
- una unidad de procesamiento (113), que puede ser en forma de microcontrolador, circuito FPGA u otro sistema de procesamiento,
- una unidad de memoria (106),
- un módulo sin contacto NFC (102),
- Bluetooth (103) u otro tipo de interfaz de comunicación inalámbrica,
- un conector de audio (104),
- una toma de audio (108),
- un micrófono (110),
- un altavoz principal (111),
- una conexión USB (101),
- un elemento de seguridad (105), adaptado para garantizar el almacenamiento seguro de datos clave y que incluye un mecanismo para evitar y detectar el acceso no autorizado al módulo de codificación de encriptado,
- un altavoz secundario (109) para bloquear un micrófono incorporado en el dispositivo de comunicación,
- una carcasa adaptada por razones de seguridad de modo que cualquier manipulación del interior del dispositivo deshabilitará su uso posterior, en donde además la carcasa está adaptada para inhabilitar el funcionamiento del micrófono del dispositivo de comunicación, en donde se proporciona un diseño estructural de la carcasa que deshabilita la captura directa de sonido mediante el dispositivo de comunicación sirviendo como barrera.

2. El módulo de codificación de encriptado según la reivindicación 1, que permite la mensajería segura, la transferencia de datos y las llamadas de voz/habla entre dos o más dispositivos/usuarios.

3. El módulo de codificación de encriptado según cualquiera de las reivindicaciones anteriores, adaptado para funcionar en combinación con una aplicación especial en el dispositivo de comunicación usado para controlar, configurar, administrar y actualizar el módulo de codificación de encriptado, en el que es característico de la comunicación entre el módulo de codificación de encriptado y la aplicación en el dispositivo de comunicación que se implementa para ser segura con el uso de codificación (encriptado).

4. El módulo de codificación de encriptado según cualquiera de las reivindicaciones anteriores, que incluye que la interfaz de comunicación entre el dispositivo de comunicación (204) y el módulo de codificación de encriptado se implementa con el uso de una interfaz USB (200) y/o tecnología de comunicación inalámbrica tal como Bluetooth (202) y/o interfaz electroacústica (203) utilizando la entrada/salida de auriculares y/o una interfaz NFC sin contacto (201) y/u otras interfaces inalámbricas, tal como banda de RF ISM, ZigBee, WiFi o IR.

5. El módulo de codificación de encriptado según cualquiera de las reivindicaciones anteriores, adaptado para ser operado sin la aplicación en el dispositivo de comunicación en un modo de operación independiente (figura 3).

6. El módulo de codificación de encriptado según cualquiera de las reivindicaciones anteriores, que está adaptado para ser utilizado para capturar y reproducir datos de audio (o voz) en su propio altavoz y micrófono internos o el(los) altavoz(es) y micrófono(s) del dispositivo de comunicación al que se está conectado, en donde también puede usarse cualquier otro dispositivo externo que sea capaz de capturar y reproducir sonido y que esté conectado al módulo de codificación de encriptado, en donde el dispositivo externo se puede conectar directamente al módulo de codificación de encriptado usando una conexión por cable (301) o inalámbrica (302), y el sistema puede utilizar cualquier combinación de los regímenes de captura y reproducción de sonido enumerados.

7. El módulo de codificación de encriptado según cualquiera de las reivindicaciones anteriores, en donde dicho módulo está integrado o conectado como un dispositivo intermediario entre el dispositivo de comunicación al que está conectado (300) y el dispositivo con capacidad de captura y/o reproducción de sonido/voz o datos/mensajes, tal como auriculares (303), en donde la conexión se implementa mediante una conexión por cable (301).

8. El módulo de codificación de encriptado de acuerdo con una de las reivindicaciones anteriores, en el que dicho módulo está integrado o conectado como una interfaz entre el dispositivo de comunicación al que está conectado (300) y otro dispositivo inalámbrico externo tal como auriculares inalámbricos (304) o radio de coche (305), en donde la conexión se implementa usando una conexión inalámbrica (302).

9. El módulo de codificación de encriptado de acuerdo con una de las reivindicaciones anteriores, **caracterizado por**

que utiliza cualquier combinación de dispositivos integrados y externos para capturar y/o reproducir sonido o para enviar y/o recibir mensajes/datos.

10. El módulo de codificación de encriptado de acuerdo con una de las reivindicaciones anteriores, **caracterizado por que** interconecta directamente dispositivos de comunicación (figura 4) o utiliza dispositivos interinos para la conexión (por ejemplo, servidor, pasarela) (figura 5) y, por lo tanto, permite un enrutamiento seguro y el establecimiento de una red segura.

Fig. 1

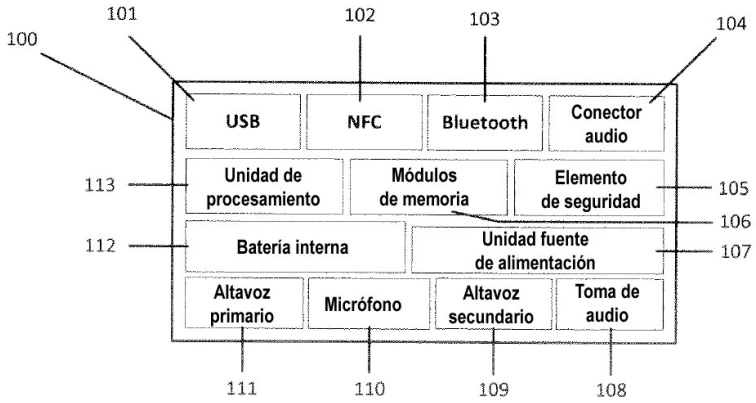


Fig. 2

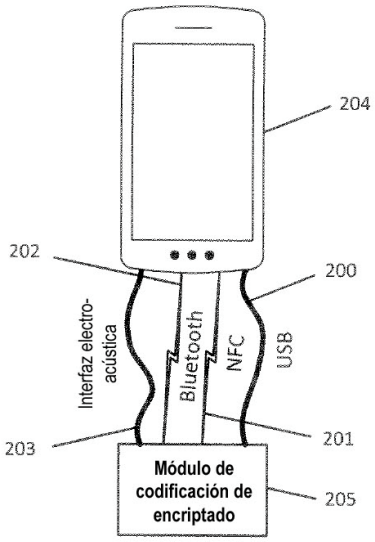


Fig. 3

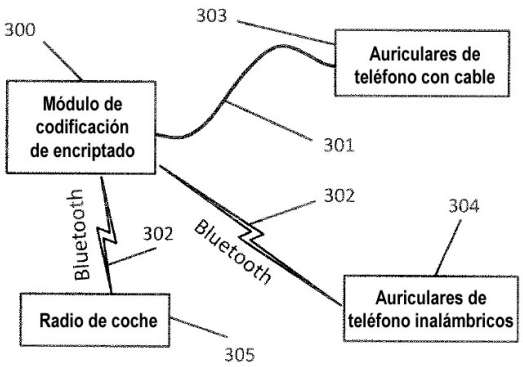


Fig. 4

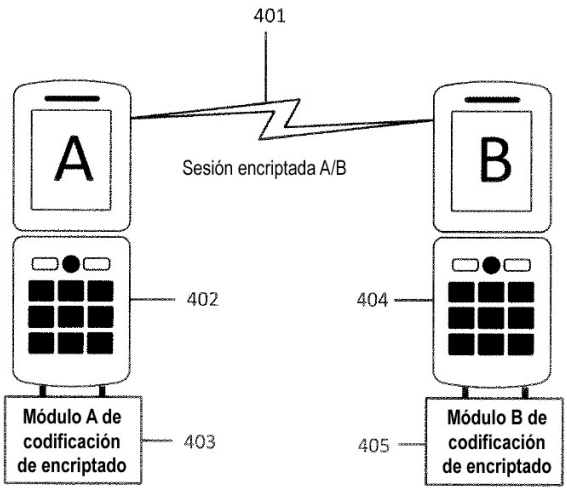

401
A
Sesión encriptada A/B
B
402
404
Módulo A de codificación de encriptado
403
405
Módulo B de codificación de encriptado

Fig.5

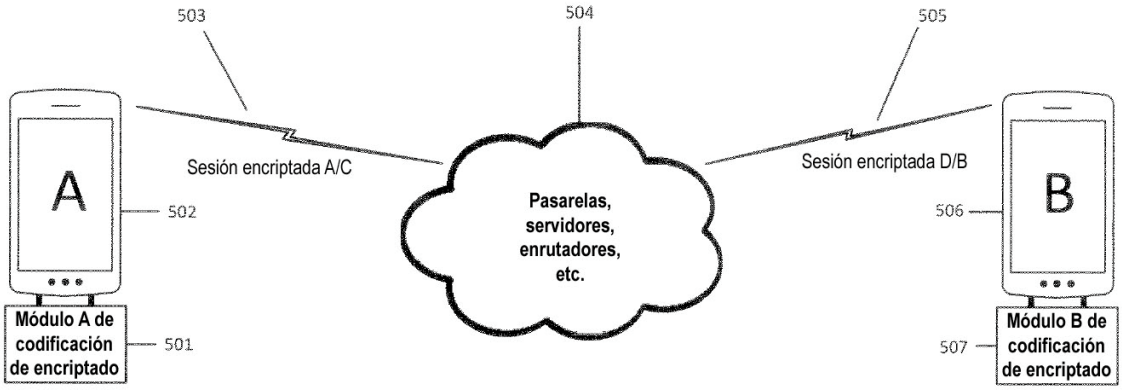

503
504
505
A
Sesión encriptada A/C
Pasarelas, servidores, enrutadores, etc.
Sesión encriptada D/B
B
502
506
Módulo A de codificación de encriptado
501
507
Módulo B de codificación de encriptado

Fig. 6

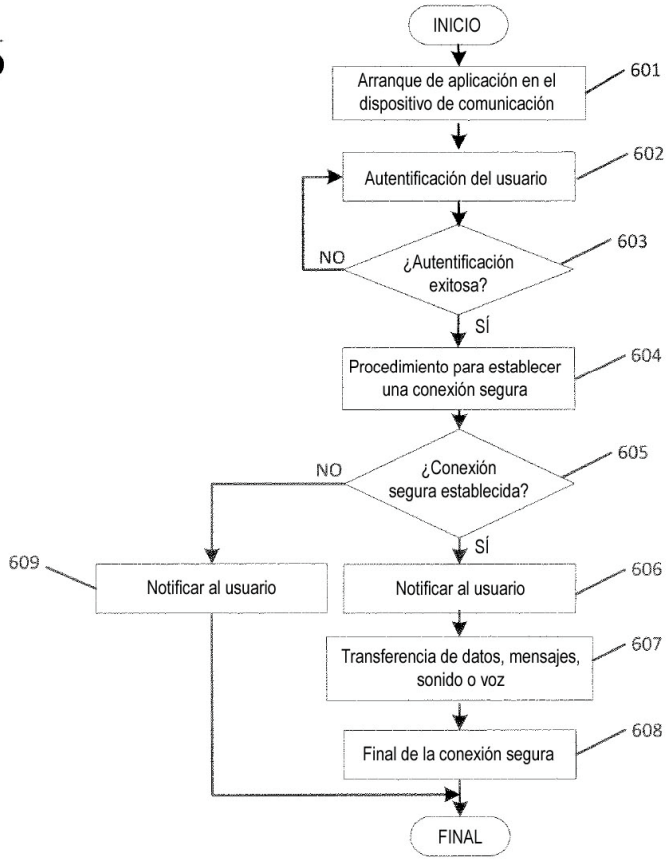

INICIO
Arranque de aplicación en el dispositivo de comunicación
601
Autentificación del usuario
602
NO
¿Autentificación exitosa?
603
SÍ
Procedimiento para establecer una conexión segura
604
NO
¿Conexión segura establecida?
605
SÍ
609
Notificar al usuario
Notificar al usuario
606
Transferencia de datos, mensajes, sonido o voz
607
Final de la conexión segura
608
FINAL

Fig. 7

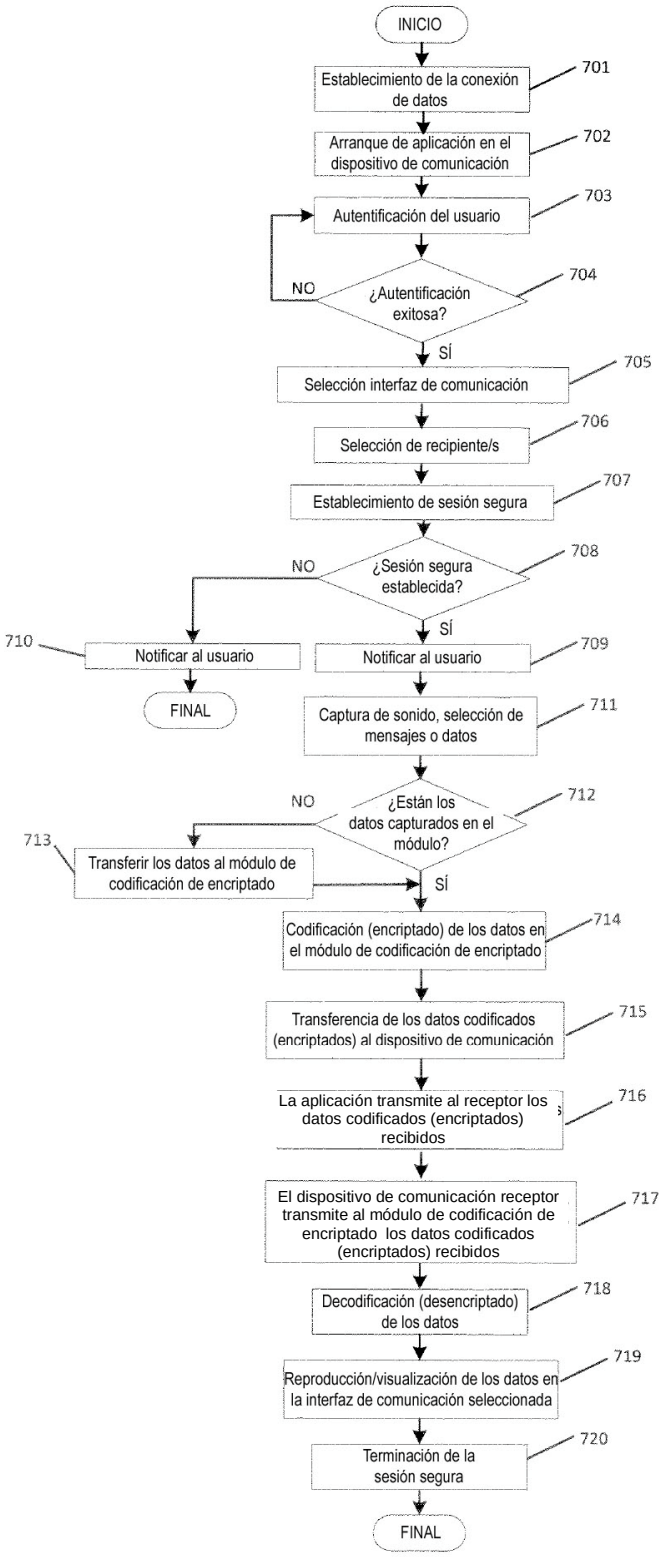

INICIO
Establecimiento de la conexión de datos
701
Arranque de aplicación en el dispositivo de comunicación
702
Autentificación del usuario
703
NO
¿Autentificación exitosa?
704
SÍ
Selección interfaz de comunicación
705
Selección de recipiente/s
706
Establecimiento de sesión segura
707
NO
¿Sesión segura establecida?
708
SÍ
710
Notificar al usuario
FINAL
Notificar al usuario
709
Captura de sonido, selección de mensajes o datos
711
NO
¿Están los datos capturados en el módulo?
712
713
Transferir los datos al módulo de codificación de encriptado
SÍ
Codificación (encriptado) de los datos en el módulo de codificación de encriptado
714
Transferencia de los datos codificados (encriptados) al dispositivo de comunicación
715
La aplicación transmite al receptor los datos codificados (encriptados) recibidos
716
El dispositivo de comunicación receptor transmite al módulo de codificación de encriptado los datos codificados (encriptados) recibidos
717
Decodificación (desencriptado) de los datos
718
Reproducción/visualización de los datos en la interfaz de comunicación seleccionada
719
Terminación de la sesión segura
720
FINAL

Fig. 8

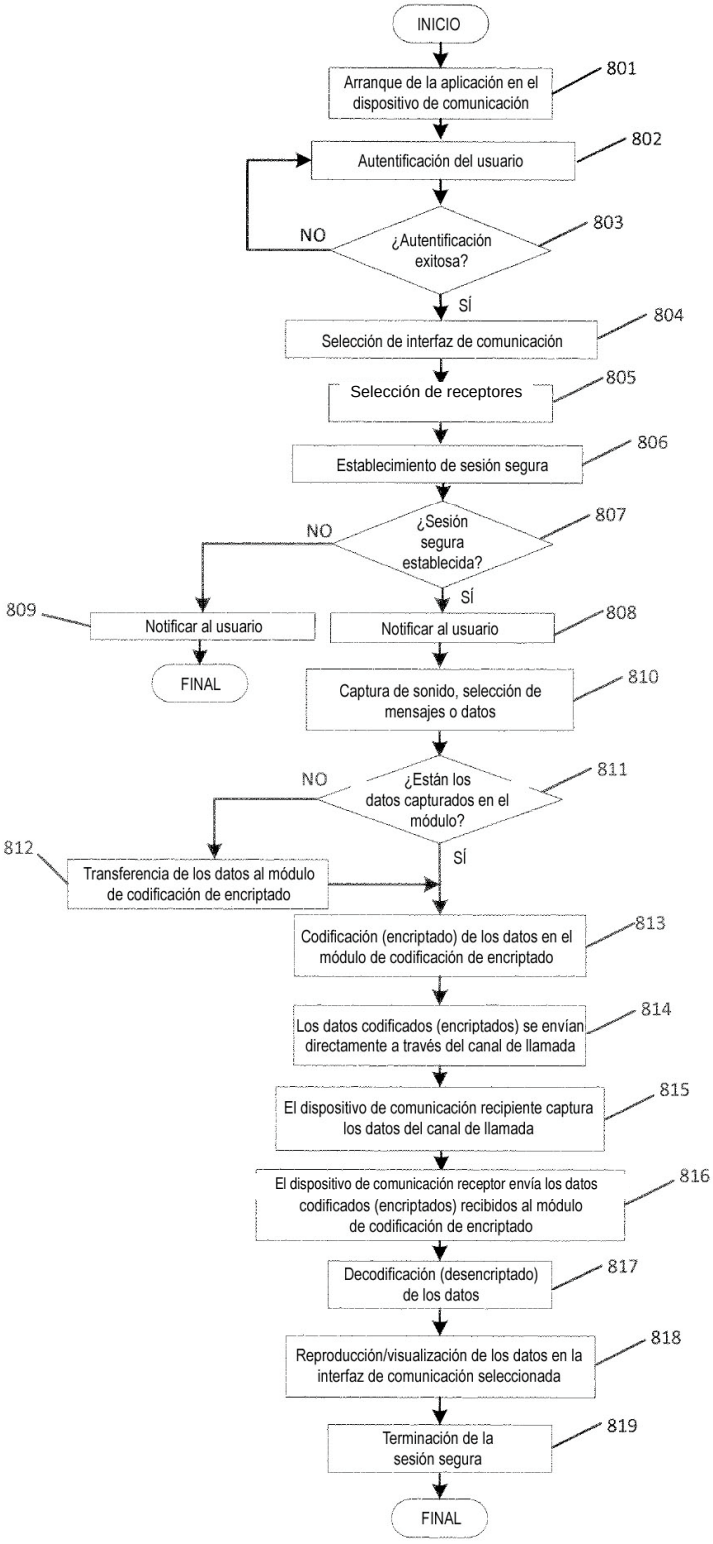

INICIO
Arranque de la aplicación en el dispositivo de comunicación
801
Autentificación del usuario
802
¿Autentificación exitosa?
803
NO
SÍ
Selección de interfaz de comunicación
804
Selección de receptores
805
Establecimiento de sesión segura
806
¿Sesión segura establecida?
807
NO
SÍ
Notificar al usuario
809
FINAL
Notificar al usuario
808
Captura de sonido, selección de mensajes o datos
810
¿Están los datos capturados en el módulo?
811
NO
SÍ
Transferencia de los datos al módulo de codificación de encriptado
812
Codificación (encriptado) de los datos en el módulo de codificación de encriptado
813
Los datos codificados (encriptados) se envían directamente a través del canal de llamada
814
El dispositivo de comunicación recipiente captura los datos del canal de llamada
815
El dispositivo de comunicación receptor envía los datos codificados (encriptados) recibidos al módulo de codificación de encriptado
816
Decodificación (desencriptado) de los datos
817
Reproducción/visualización de los datos en la interfaz de comunicación seleccionada
818
Terminación de la sesión segura
819
FINAL

Fig. 9

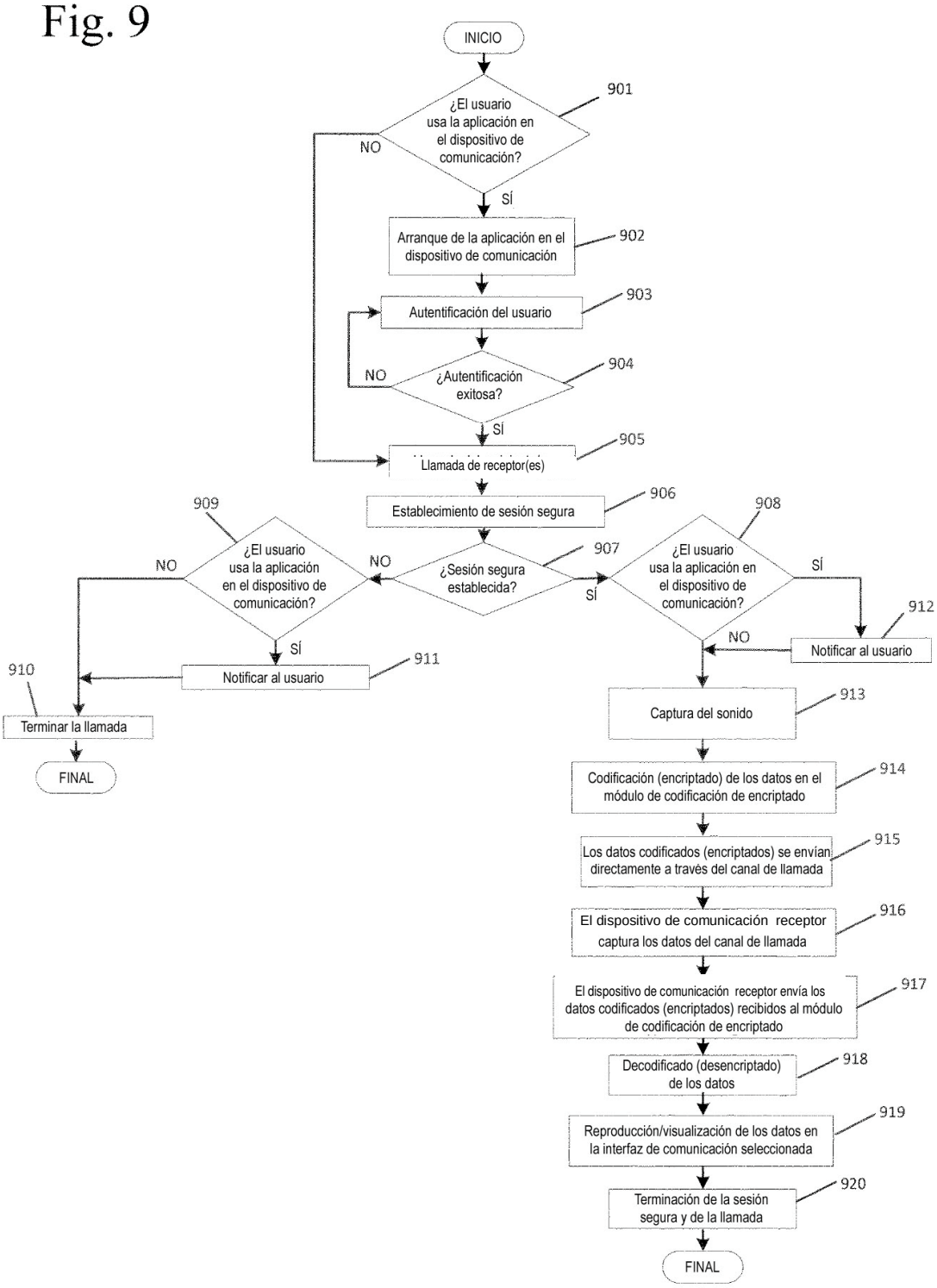

INICIO
¿El usuario usa la aplicación en el dispositivo de comunicación?
901
NO
SÍ
Arranque de la aplicación en el dispositivo de comunicación
902
Autentificación del usuario
903
¿Autentificación exitosa?
904
NO
SÍ
Llamada de receptor(es)
905
Establecimiento de sesión segura
906
¿Sesión segura establecida?
907
NO
SÍ
¿El usuario usa la aplicación en el dispositivo de comunicación?
908
SÍ
NO
Notificar al usuario
912
¿El usuario usa la aplicación en el dispositivo de comunicación?
909
NO
SÍ
Notificar al usuario
911
Terminar la llamada
910
FINAL
Captura del sonido
913
Codificación (encriptado) de los datos en el módulo de codificación de encriptado
914
Los datos codificados (encriptados) se envían directamente a través del canal de llamada
915
El dispositivo de comunicación receptor captura los datos del canal de llamada
916
El dispositivo de comunicación receptor envía los datos codificados (encriptados) recibidos al módulo de codificación de encriptado
917
Decodificado (desencriptado) de los datos
918
Reproducción/visualización de los datos en la interfaz de comunicación seleccionada
919
Terminación de la sesión segura y de la llamada
920
FINAL

Fig. 10

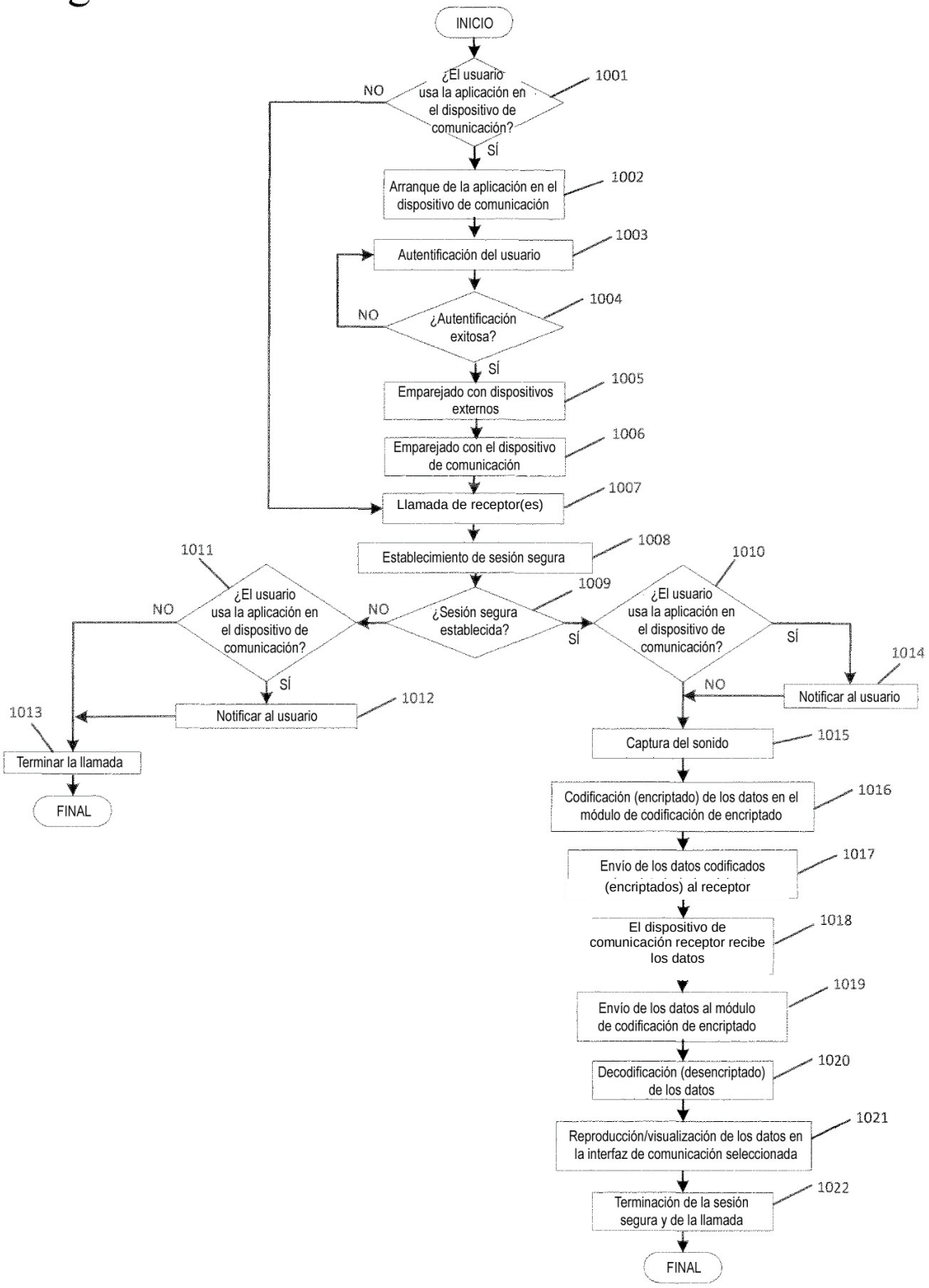
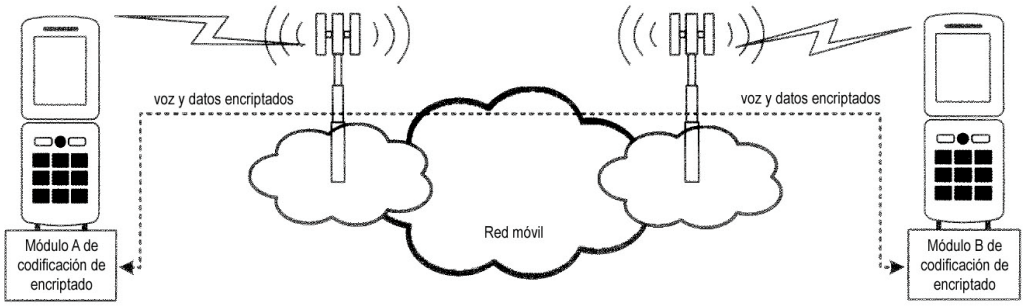

INICIO
¿El usuario usa la aplicación en el dispositivo de comunicación?
1001
NO
SÍ
Arranque de la aplicación en el dispositivo de comunicación
1002
Autentificación del usuario
1003
¿Autentificación exitosa?
1004
NO
SÍ
Emparejado con dispositivos externos
1005
Emparejado con el dispositivo de comunicación
1006
Llamada de receptor(es)
1007
Establecimiento de sesión segura
1008
¿Sesión segura establecida?
1009
NO
SÍ
¿El usuario usa la aplicación en el dispositivo de comunicación?
1010
SÍ
NO
Notificar al usuario
1014
¿El usuario usa la aplicación en el dispositivo de comunicación?
1011
NO
SÍ
Notificar al usuario
1012
1013
Terminar la llamada
FINAL
Captura del sonido
1015
Codificación (encriptado) de los datos en el módulo de codificación de encriptado
1016
Envío de los datos codificados (encriptados) al receptor
1017
El dispositivo de comunicación receptor recibe los datos
1018
Envío de los datos al módulo de codificación de encriptado
1019
Decodificación (desencriptado) de los datos
1020
Reproducción/visualización de los datos en la interfaz de comunicación seleccionada
1021
Terminación de la sesión segura y de la llamada
1022
FINAL

Fig. 11


voz y datos encriptados
voz y datos encriptados
Red móvil
Módulo A de codificación de encriptado
Módulo B de codificación de encriptado