(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 616 116**

(21) Número de solicitud: 201630957

(51) Int. CI.:

H04W 12/02 (2009.01)

(12) PATENTE DE INVENCIÓN B1

(22) Fecha de presentación:

13.07.2016

(43) Fecha de publicación de la solicitud:

09.06.2017

Fecha de la concesión:

22.03.2018

(45) Fecha de publicación de la concesión:

02.04.2018

(73) Titular/es:

DÍAZ BAÑO , Álvaro (50.0%)
GRAN VIA LES CORTS CATALANES, 996, 4º 2ª
08018 BARCELONA (Barcelona) ES y
DÍAZ BAÑO, Pablo (50.0%)

(72) Inventor/es:

DÍAZ BAÑO , Álvaro y
DÍAZ BAÑO , Pablo

(54) Título: **DISPOSITIVO PORTÁTIL DE CIFRADO DE AUDIO MEDIANTE PROTOCOLO TLS**

(57) Resumen:
Dispositivo portátil de cifrado de audio mediante protocolo TLS.
Se dispone de una memoria no volátil (23) certificados electrónicos x509 v3 (22) de los terminales de comunicación (10); el certificado electrónicos x509 v3 (22) y los bytes de la clave privada (19) del propio dispositivo; ensambla conectores de audio, físicos o inalámbricos, y electrónica para ser identificado como unos auriculares externos con micrófono; dispone de una memoria no volátil (23) que almacena la lógica informática (16) y los algoritmos criptográficos necesarios para establecer una comunicación segura mediante protocolo TLS; un procesador (7) que realiza los procesos criptográficos de autenticación TLS y cifrado de las comunicaciones mediante protocolo TLS, descifrando la señal digital recibida y cifrando el señal digital enviada; y un procesador de señal de audio (6) que realiza conversión de señal de audio analógico/digital y digital/analógico, y canaliza la comunicación por los canales de reproducción o transmisión.

ES 2 616 116 B1

DESCRIPCIÓN

Dispositivo portátil de cifrado de audio mediante protocolo TLS

SECTOR DE LA TÉCNICA

La presente invención pertenece al sector de la seguridad de las comunicaciones.

Se refiere a un nuevo dispositivo electrónico que al ser conectado a un terminal de comunicación hace posible realizar una autenticación mutua con otro terminal de comunicación, y cifrar las comunicaciones empleando protocolo Transpor Layer Security (TLS).

Más particularmente, la presente invención se refiere a un dispositivo que permite almacenar el certificado electrónico x509 v3 del usuario del terminal y los bytes de su clave privada, y el certificado electrónico x509 v3 del terminal de comunicación con el que desea establecer comunicación confidencial, y utilizar la clave privada y la clave pública contenida en los certificados electrónicos para establecer comunicación segura mediante protocolo TLS. Cada dispositivo que interviene en la comunicación dispone de un procesador digital de señal que posee un conjunto de instrucciones, un hardware y un software optimizados para aplicaciones que requieren operaciones numéricas de muy alta velocidad, como convertir la señal de audio de analógica a digital, cifrado y descifrado del audio, y conversión de la señal de digital a analógica.

Es pues objeto de la invención proveer al usuario de un dispositivo autónomo y portátil, que al ser conectado a terminales de comunicaciones permite realizar una autenticación mutua de las partes y cifrado de sus comunicaciones. El dispositivo dispone de conectores que permiten asociarlo a un terminal de comunicación, y a un auricular con micrófono.

ANTECEDENTES DE LA INVENCIÓN

Aunque existen diferentes procedimientos para salvaguardar la privacidad de las comunicaciones todos ellos, al estar integrados en el propio terminal de comunicación, tienen la limitación de que:

1- la tecnología hacker actual permite capturar la comunicación en el mismo instante en que es capturada por el micrófono ensamblado en el terminal de comunicación, es decir, antes de que la voz llegue al sistema de seguridad; y captura el audio del altavoz integrado en el terminal, es decir después de que el sistema de seguridad haya descifrado el audio recibido. Por lo tanto, de nada sirve que sea segura la comunicación entre los terminales, los hacker la capturan fuera del contexto de seguridad.

Se ha realizado un amplio estudio sobre las patentes existentes, y ninguna de ellas describe los métodos reivindicados en esta invención. Concretamente:

La publicación “ModerneVerfahren der Kryptographie” (“Procedimientos modernos de criptografía”) Beutelspacher, Schwenk, Wolfenstetter, 3. Edición, 1999, ViewegVerlag, contiene una descripción detallada de los procedimientos criptográficos de clave pública.

El sistema criptográfico RSA que se describe en la Patente de EE.UU. Nº 4.405.829 concedida a Rivest y otros describe un ejemplo de metodología de un sistema criptográfico de clave pública.

EXPLICACIÓN DE LA INVENCIÓN

La invención que aquí se describe viene a resolver la problemática anteriormente expuesta, concibiendo un dispositivo constituido a partir de un soporte electrónico, tal como una pequeña mochila o una placa de circuito integrado ensamblada en el interior del terminal, que comprende los siguientes elementos:

1. Al menos un par de claves del dispositivo, pública y privada; y la clave pública del dispositivo con el que se quiere establecer comunicación confidencial; los algoritmos criptográficos necesarios para cifrar las comunicaciones.

Las claves públicas (20) y (21) pueden estar contenidas en certificados electrónicos X509 v3 (22) según estándar UIT-T, o sus bytes almacenados en un contenedor de información estructurada como por ejemplo un XML o una base de datos, debidamente etiquetados con el identificador que comparten con su clave privada (19). O pueden están almacenadas en los contenedores de seguridad de

un chip criptográfico.

2. Medios de almacenamiento informático, donde se guardan las claves, y los algoritmos criptográficos necesarios.

Los medios de almacenamiento pueden ser del tipo EEPROM, o del tipo EPROM, o cualquier otro tipo de memoria no volátil.

3. Un medio que permita la conexión del dispositivo con el terminal de comunicación, de tal forma que sea reconocido como un auricular con micrófono externo con el fin de que el terminal de comunicación transfiera la señal de audio por el canal correspondiente al conector del dispositivo.

4. Un medio que permita conectar al dispositivo un auricular con micrófono, salvo que en el propio dispositivo se haya integrado un auricular y un micrófono.

Los medios de conexión pueden ser físicos como por ejemplo un jack, un mini usb, o conectores propios del fabricante como MFI (Madefor iPhone/iPad/iPod); o inalámbricos, como por ejemplo Bluetooth, Wifi.

5. Medios de procesamiento informático asociados a los medios de almacenamiento y a los medios de conexión; estando programados para realizar comunicaciones confidenciales mediante tecnología TLS (Transport Layer Security), y la conversión de la señal analógica/digital y digital/analógica.

El procedimiento TLS es un protocolo definido en la RFC 5246 de Internet EngineeringTaskForce (IETF), emplea criptografía asimétrica para autentificar a la contraparte con quien se está comunicando, e intercambiar una llave simétrica (clave de sesión) en un contexto conocido como “perfect forward secrecy” (FPS) que garantiza que el descubrimiento de las claves utilizadas actualmente no compromete la seguridad de las claves usadas con anterioridad. Esta sesión es luego usada para cifrar la comunicación entre las partes.

Los medios de procesamiento de la señal requieren tener en consideración que la señal analógica adquirida por un micrófono de un teléfono celular GSM, es muestreada a 8 kHz, con 13 bits por muestra, lo que equivale a 104 000 bit/s.

Según la calidad deseada o disponible, la salida de los codecs reduce el ancho de banda a un rango entre 4,75 kbit/s y 13 kbit/s, es decir, permiten factores de compresión de 21 a 8 veces, por lo tanto, es necesario convertir la señal de analógica a digital antes de su procesado, y una vez cifrada o descifrada, convertirla de digital a analógica, para ello es necesario utilizar algoritmos complejos que requieren alta capacidad de proceso, por ello el dispositivo de esta invención incluye un procesador digital de señal (DSP), el cual puede estar asociado a un procesador criptográfico que reforzaría la seguridad, al almacenar de forma segura las claves y mejoraría los tiempos de proceso criptográfico al contar con un procesador dedicado, liberando al DSP de esta función.

Para la alimentación de los elementos electrónicos descritos, el dispositivo caso de conectarse físicamente con el terminal de comunicación, puede emplear el propio flujo eléctrico que recibe el conector; si la conexión es inalámbrica o si el consumo de los componentes lo hace necesario o recomendable, el dispositivo puede integrar una fuente de energía eléctrica (pilas o batería recargable y sustituibles) o bien una fuente de energía renovable (pequeñas placas fotovoltaicas insertadas en el soporte con el que se construye el dispositivo)para conferirle autonomía y portabilidad.

Las ventajas que ofrece el dispositivo propuesto frente a los actuales sistemas de seguridad integrados en la electrónica del terminal de comunicación, son:

- Seguridad reforzada, este dispositivo es compatible con los actuales sistemas de privacidad que estén implantados en los terminales de comunicación. El hacker deberá quebrantar dos niveles de seguridad, la que tenga integrada el terminal de comunicación, y la de este dispositivo.
- Al conectar el dispositivo de esta invención al terminal de comunicación, y ser reconocido como un accesorio de audio y micro externo, el terminal de comunicación deshabilita el canal de su altavoz y micrófono, imposibilitando cualquier ataque que pretendiera hacer uso de esos componentes.
- El dispositivo es autónomo y portable, interoperable con cualquier terminal de comunicación con el único requerimiento que simplemente disponga de un conector compatible. Para ampliar el espectro de equipos interoperables se pueden hacer uso de adaptadores, cuya oferta actual cubre prácticamente el 100 % de los modelos existentes en el mercado.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Para complementar la descripción que se está realizando y con objeto de ayudar a una mejor comprensión de las características de la invención, se acompaña como parte integrante de dicha descripción un juego de dibujos, en los que se ha representado lo siguiente:

Figura 1 ilustra un conector Jack para conexión Open Mobile Terminal Platform (OMTP).

Figura 2 ilustra unos auriculares con micrófono y Jack (OMTP).

Figura 3 ilustra un esquema del dispositivo sin carcasa, que ensambla conectores físicos (OMTP).

Figura 4 ilustra un esquema de procesamiento digital de una señal analógica a digital y de digital a analógica, con cifrado de la comunicación.

REALIZACIÓN PREFERENTE DE LA INVENCIÓN

Una realización preferente del sistema aquí descrito, comprende esencialmente, los siguientes elementos:

a) Dos terminales de comunicación (10), que disponen de un conector hembra (9) para jack macho tipo OMTP miniaturizado de 3,5 mm (8), se ha elegido un Smartphone Galaxy S5 de Samsung.

b) Dos auriculares con micrófono (5) que tienen un conector jack macho tipo OMTP miniaturizado de 3,5 mm (8) con cuatro canales: audio izquierdo (1), audio derecho (2), micrófono (3), masa (4).

c) Dos dispositivos de cifrado TLS (11) que ensamblan cada uno de ellos, un conector hembra (9) para jack macho tipo OMTP miniaturizado de 3,5 mm (8), un conector jack macho tipo OMTP miniaturizado de 3,5 mm (8) con canal de audio izquierdo (1) canal de audio derecho (2), canal de micrófono (3) canal masa (4), asociados todos ellos a la electrónica necesaria para que el dispositivo de cifrado (11) sea identificado por el terminal de comunicación (10) como un auricular con micrófono (5), el esquema de esta realización preferente, al tratarse de una conexión física que tiene conectado a su vez un auricular con micrófono, hace que esta identificación se produzca automáticamente sin necesidad de otros elementos complementarios. No obstante si la conexión fuera inalámbrica u empleara otro

tipo de conector, tampoco presupondría reto técnico relevante, hay extensa documentación y esquemas en internet que detallan distintos modelos de realización; un procesador digital de señal (DSP) (6), se ha elegido un procesador de doble núcleo de alto rendimiento DSP / MCU audio de Texas Instruments modelo TAS3204 con interfaz analógica, se trata de un sistema-en-chip de audio (SOC) que consiste en un procesador de audio totalmente programable, un 3:1 estéreo MUX de entrada analógica, cuatro ADCs, cuatro DACs, y otra funcionalidad analógica, con consumo de 3.4 V y reguladores integrados; aunque no es imprescindible, sí que es una mejora funcional la inclusión de un procesador criptográfico (7), se ha elegido para esta realización preferente el procesador del fabricante NXP el modelo J3D145_M59,este procesador dispone de capacidad de proceso matemático, algoritmos criptográficos: cifrado asimétrico, cifrado simétrico, generación aleatoria de números, con consumo de 3,6 V. y ensambla memoria no volátil (23) que permite almacenar certificados x509 v3 (22)con la clave pública del dispositivo (20) y la clave pública del dispositivo al que se conecta (21), y los bytes de la clave privada del dispositivo (19). Existe extensa documentación en internet con esquemas electrónicos con placas de circuito impreso que ensamblan conectores de audio (8) y (9), microprocesadores criptográficos (7) y procesadores de señal de audio (6), aunque ninguno asociando un microprocesador criptográfico (7) y un procesadores de señal de audio (6), esta conexión no presupone reto técnico alguno, solo requiere conectar los canales de transmisión de datos de ambos procesadores.

d) Lógica informática (16) programada en lenguaje C almacenada en la memoria no volátil (23), que incorpora protocolo TLS para realizar autenticación mutua de los dispositivos, el cifrado de las comunicaciones, y los algoritmos de conversión de señal. Existe extensa documentación en Internet, con código fuente de libre uso, para integrar protocolo TLS.

Se realiza el siguiente procedimiento:

1. Se conectan los auriculares con micrófono (5) a sus respectivos dispositivos de cifrado (11), introduciendo el jack macho (8) del auricular con micrófono (5) al conector hembra (9) del dispositivo de cifrado (11);

2. Se conectan los dispositivos de cifrado (11) a sus respetivos terminales de

comunicación (10), introduciendo el jack macho (8) del dispositivo de cifrado (11) al conector hembra (9) del Terminal de Comunicación (10), la conexión física del jack macho (8) deshabilita automáticamente el altavoz y el micrófono del terminal de comunicación (10);

3. El terminal de comunicación A (10A) realiza una llamada al terminal de comunicación B (10B), se establece la comunicación, y el programa (16) realiza el siguiente procedimiento:

a) Mediante el protocolo TLS se realiza el proceso de autenticación mutua de los dispositivos de cifrado y el intercambio de la clave de sesión, mediante el empleo de los certificados electrónicos y clave privada de sus respectivos terminales. La clave pública se emplea para cifrar la clave de sesión, y la privada se emplea para descifrarla.

b) La clave de sesión es empleada para cifrar y descifrar las comunicaciones.

c) La señal de entrada analógica (12) se canaliza al convertidor Analógico / Digital (14), el Procesador Digital de Señal (6) descifra la señal de audio digital recibida (17), y cifra la señal de audio digital a enviar (18), canaliza el audio procesado al convertidor Digital/Analógico (15); según la lógica de programación desarrollada, también podría ser posible que el microprocesador criptográfico asumirá el proceso de cifrado y descifrado de la señal de audio digital.

d) Las señal de audio descifrada (17) la canaliza a los canales de audio (1) y (2) de los respectivos Jack (8); la señal de audio cifrada (18) la canaliza al canal de audio (3) de los respectivos Jack (8).

REIVINDICACIONES

1.- Dispositivo portátil de cifrado de audio mediante protocolo TLS, caracterizado porque comprende:

Paso 1: Una memoria no volátil (23) que almacena el certificado electrónico x509 v3 (22) que contiene las clave pública (21) del terminal de comunicación (10) con los que se establece comunicación segura; el certificado electrónico x509 v3 (22) que contiene la clave pública (20) y los bytes de la clave privada (19) del propio dispositivo.

Paso 2: El dispositivo de cifrado (11) ensambla conectores de audio, físicos o inalámbricos, con la electrónica necesaria para ser identificado por el terminal de comunicación (10) como unos auriculares externos con micrófono; y un procesador digital de señal (6) que dispone de la capacidad para convertir la señal de audio analógico/digital (14) y digital/analógico (15).

Paso 3: En la memoria no volátil (23) almacena la lógica informática (16) y los algoritmos criptográficos necesarios para establecer una comunicación segura mediante protocolo TLS; el procesador digital de señal (6) realiza los procesos criptográficos de autenticación TLS y cifrado de las comunicaciones mediante protocolo TLS, descifrando la señal digital recibida y cifrando la señal digital a transmitir, y, una vez procesada, canaliza la comunicación de audio por los canales de reproducción (1) (2) y transmisión (3) correspondientes.

2.- Dispositivo portátil de cifrado de audio mediante protocolo TLS, según la Reivindicación 1, caracterizado porque en el Paso 3 comprende además:

Un microprocesador criptográfico (7) que incorpora memoria no volátil (23) que almacena la lógica informática (16) y los algoritmos criptográficos necesarios para establecer una comunicación segura mediante protocolo TLS; este procesador (7) realiza la autenticación mutua de los dispositivos que intervienen en la comunicación, recibe la señal digital del procesador digital de señal (6), descifra la señal recibida y cifra la señal a transmitir, y ambas señales son canalizadas al procesador digital de señal (6).

3.- Dispositivo portátil de cifrado de audio mediante protocolo TLS según Reivindicación 1, caracterizado porque en el Paso 1 es sustituido por:

Una memoria no volátil (23) que almacena un fichero de información estructurada que contiene los bytes de las claves públicas (21) de los terminales de comunicación (10) con los que se establece comunicación segura, y los identificadores que comparte con sus respectivas claves privadas; además contiene los bytes de la clave pública (20), los bytes de la clave privada (19) del propio dispositivo, y el identificador que comparten.

4.- Dispositivo portátil de cifrado de audio mediante protocolo TLS según Reivindicación 1, caracterizado porque en el Paso 3 comprende además previamente:

a) Un módulo reconocedor de voz/habla. Reconocimiento de la voz y el habla respetivamente.
b) En la memoria no volátil se almacena una identidad de voz, y diferentes órdenes.
c) La lógica informática (16) se amplía con la capacidad de reproducir voz sintetizada y reconocer contestaciones, aplicando diferentes variables según las contestaciones recibidas. Este método permite, entre otras utilidades, solicitar PIN para activar el dispositivo de cifrado, verificar que la voz corresponde al usuario autorizado.

5.- Dispositivo portátil de cifrado de audio mediante protocolo TLS según Reivindicación 1, caracterizado porque en el Paso 1 es sustituido por a) y el Paso 3 comprende además previamente b):

a) Una memoria no volátil (23) que almacena varios certificados electrónicos x509 v3 (22) que contienen las claves públicas (21) asociadas a los terminales de comunicación (10) con los que se establece comunicación segura; contiene varios certificados electrónicos x509 v3 (22) que contienen las claves públicas (20) y los bytes de las claves privadas (19) asociadas a esas claves públicas.
b) La lógica de informática (16) incluye un interfaz de usuario en el terminal de comunicación (10) y un procedimiento por el cual, previamente a establecer la

comunicación, el usuario mediante el interfaz instalado en el terminal de comunicación (10), selecciona el certificado digital x509 v3 (22) que desea activar en su dispositivo (11) para establecer comunicación; al establecer la comunicación la lógica de informática (16) determina si el certificado x509 v3 (2) del terminal de comunicación (10) remoto está cargado o no en la memoria no volátil (23) del dispositivo (11), si no está cargado mediante el interfaz de usuario, se da la posibilidad de aceptarlo en cuyo caso el certificado electrónico x509 v3 (22) del dispositivo (11) remoto es cargado en la memoria no volátil (23) del dispositivo (11).

6.- Dispositivo portátil de cifrado de audio mediante protocolo TLS según Reivindicación 1, en combinación con la Reivindicación 5 b), caracterizado porque en el Paso 3 comprende además previamente:

La lógica informática (16) incluye la capacidad del leer el UUID de los componentes electrónicos del terminal de comunicación (10) al que se conecta; el interfaz de usuario permite registrar en la memoria no volátil (23) los UUID de aquellos terminarles de comunicación (10) en los que puede ser utilizado el dispositivo (11), y previo a que se active el dispositivo (11), la lógica informática lee el UUID del terminal de comunicación (10) y determina si está autorizado o no a emplear el dispositivo (11).

7.- Dispositivo portátil de cifrado de audio mediante protocolo TLS según Reivindicación 1, caracterizado porque en el Paso 3 comprende además previamente:

La lógica informática (16) necesaria para que en el proceso de autenticación realizado mediante el protocolo TLS, la comunicación entre los dos terminales de comunicación (10) no se realice conversión de señal y toda la comunicación sea realizada en modo digital, reduciendo de esta forma la carga de proceso.

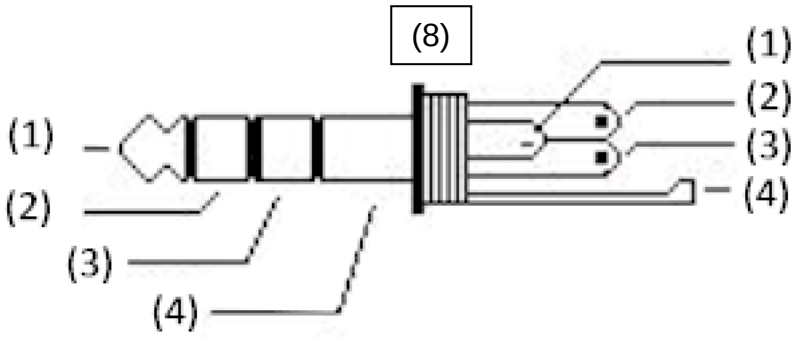

Figura 1

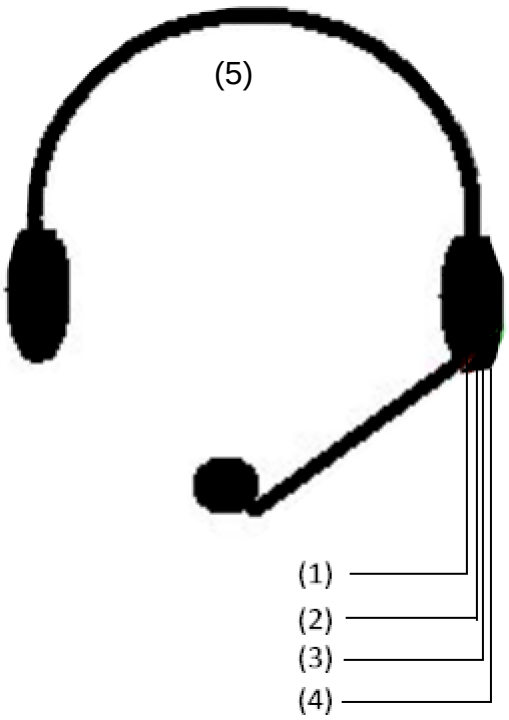

Figura 2

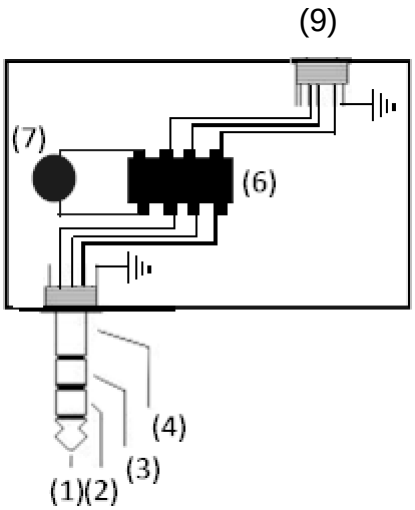

Figura 3

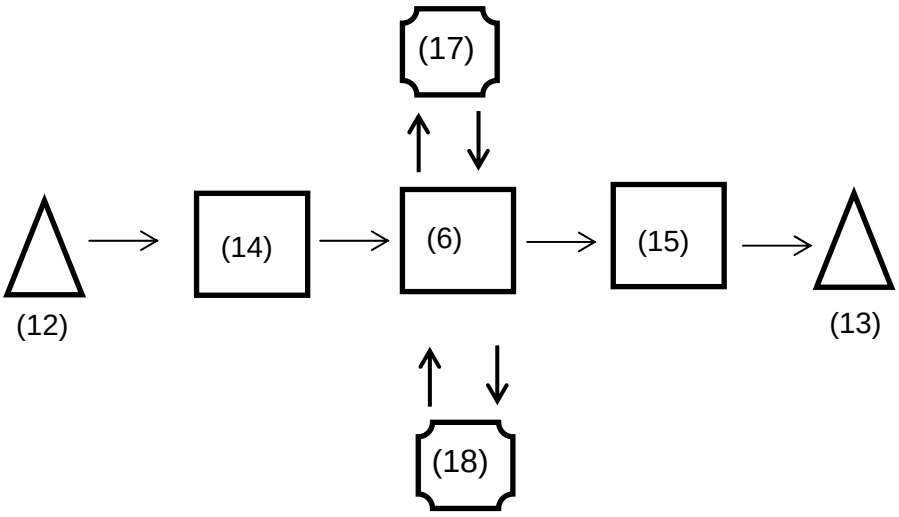

Figura 4

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201630957

(22) Fecha de presentación de la solicitud: 13.07.2016

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***H04W12/02*** (2009.01)

DOCUMENTOS RELEVANTES

Categoría	**(56) Documentos citados**	**Reivindicaciones afectadas**
X	WO 2008129546 A2 (GITA TECHNOLOGIES LTD et al.) 30/10/2008; Resumen; Descripción, página 7 líneas13-27; figuras 1-2	1-7
A	US 2003131230 A1 (CROSS GARY J) 10/07/2003, Todo el documento.	1-7
A	CN 105338475 A (THIRD RES INST MINI PUBL SECU) 17/02/2016, Todo el documento.	1-7
A	US 2016021541 A1 (HADDAD WALEED SAMI et al.) 21/01/2016, Todo el documento.	1-7
A	WO 9937108 A1 (MATRA NORTEL COMMUNICATIONS) 22/07/1999, Todo el documento.	1-7

Categoría de los documentos citados
X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	**Examinador**	**Página**
31.05.2017	**M. Muñoz Sanchez**	1/4

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

H04L, H04W

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI

Fecha de Realización de la Opinión Escrita: 31.05.2017

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-7	**SI**
	Reivindicaciones		**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones		**SI**
	Reivindicaciones	1-7	**NO**

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión.-

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

1. Documentos considerados.-

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	WO 2008129546 A2 (GITA TECHNOLOGIES LTD et al.)	30.10.2008
D02	US 2003131230 A1 (CROSS GARY J)	10.07.2003
D03	CN 105338475 A (THIRD RES INST MINI PUBL SECU)	17.02.2016
D04	US 2016021541 A1 (HADDAD WALEED SAMI et al.)	21.01.2016
D05	WO 9937108 A1 (MATRA NORTEL COMMUNICATIONS)	22.07.1999

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

Se considera D01 el documento más próximo del estado de la técnica al objeto de la solicitud.

Reivindicaciones independientes

Reivindicación 1: El documento D01 divulga un dispositivo portátil de cifrado de audio incorporado a unos auriculares con micrófono para cifrar las comunicaciones extremo a extremo a través de una red de telefonía móvil. El cifrado se hace en un extremo y el descifrado en el otro transmitiéndose el audio cifrado a través de terminales móviles.
La conexión entre los auriculares externos y los terminales móviles se hace mediante Bluetooth, por infrarrojos o un cable (Resumen; Descripción, página 7 líneas 13-27, figuras 1-2), por ejemplo. La diferencia entre el documento D01 y la reivindicación 1 es que el cifrado utilizado es en concreto TLS. Esta diferencia es una mera alternativa habitual que el experto en la materia consideraría y, por tanto, evidente para él.
Por tanto, el documento D01 afecta a la actividad inventiva de la reivindicación 1 según el art. 8.1 de la Ley de Patentes.

Reivindicaciones dependientes

Reivindicaciones 2-7: las operaciones y componentes reivindicados (autenticación mutua entre dispositivos, autorización de uso, conversión/no conversión de señal, almacenamiento de claves y lógica de operación) son elementos habituales que el experto en la materia consideraría incluir siempre y, por tanto, evidentes para él.
Así, el documento D01 también afecta a la actividad inventiva de las reivindicaciones 2-7 según el art. 8.1 de la Ley de Patentes.