(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 884 178**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04M 1/60 (2006.01)
H04M 1/253 (2006.01)
H04M 1/00 (2006.01)
H04W 4/80 (2008.01)
H04W 12/037 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **03.06.2016 PCT/EP2016/062578**

(87) Fecha y número de publicación internacional: **08.12.2016 WO16193404**

(96) Fecha de presentación y número de la solicitud europea: **03.06.2016 E 16726595 (8)**

(97) Fecha y número de publicación de la concesión europea: **04.08.2021 EP 3304850**

(54) Título: **Métodos y sistemas para la organización de sesiones de comunicación en nombre de puntos finales criptográficos**

(30) Prioridad:

04.06.2015 US 201514730807

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.12.2021

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
22-24, route de Genève
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es:

PERRINE, JÉRÔME;
BENOIT, BERNARD;
VAN RIEK, MAURICE y
OSEN, KARL

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Métodos y sistemas para la organización de sesiones de comunicación en nombre de puntos finales criptográficos

Referencia cruzada a solicitudes relacionadas

Esta solicitud reivindica la prioridad de la solicitud de U.S. No. 14/730,807, presentada el 4 de junio de 2015, titulada "METHOD AND SYSTEMS FOR COMMUNICATION-SESSION ARRANGEMENT ON BEHALF OF CRYPTOGRAPHIC ENDPOINTS."

Antecedentes

Las personas se comunican de forma inalámbrica y sobre la marcha. Entre los dispositivos que lo hacen posible se encuentran los que a veces se denominan dispositivos móviles personales. Ejemplos de dispositivos móviles personales incluyen teléfonos celulares, teléfonos inteligentes, walkie-talkies y puntos de acceso portátiles, entre otros. Un dispositivo móvil personal podría ser de mano (como puede ser el caso de un walkie-talkie), montado en la carrocería o unido a un vehículo (tal como el techo de un automóvil), por ejemplo.

Dada la relativa facilidad con la que se pueden interceptar las señales de radio, la comunicación con (o entre) dispositivos móviles personales a menudo se encripta para evitar la interceptación de la comunicación por parte de terceros. El encriptado es el proceso de convertir la voz audible u otros datos en voz ininteligible, mientras que el desencriptado es el proceso de convertir la voz ininteligible de nuevo en la voz audible original. Los algoritmos respectivos utilizados para el encriptado y el desencriptado a menudo se denominan en conjunto como un cifrado. Ejemplos de cifrados comunes incluyen estándar de encriptado avanzado (AES), Blowfish, algoritmo de encriptado de datos triple (3DES) y RC4, entre muchos otros.

El documento GB2388279A divulga un dispositivo de interfaz de audio operable para proporcionar una señal para controlar un teléfono para comunicarse con una red a través de un canal de datos, y para muestrear y encriptar señales de audio o señales derivadas del mismo antes de proporcionarlas para su transmisión por el canal de datos.

El documento EP2175580A1 divulga un auricular inalámbrico que comprende un micrófono, un altavoz, un transmisor inalámbrico para transmisión inalámbrica de señales con un dispositivo remoto, memoria para almacenar una clave de encriptado de un solo uso y una parte de encriptado para encriptar señales de voz.

El documento WO2008/129546A2 divulga unos auriculares para su uso con un teléfono que incluye una carcasa, un altavoz para audífonos, un micrófono, un procesador de encriptado y una unidad de interfaz telefónica.

Visión general

La presente invención está definida por las reivindicaciones independientes 1 y 13 adjuntas. Las realizaciones se exponen en las reivindicaciones dependientes.

Breve descripción de los dibujos

En este documento se describen diversas realizaciones de ejemplo con referencia a los siguientes dibujos, en los que numerales similares indican entidades similares, y en los que:

La figura 1 representa un sistema de comunicación, de acuerdo con al menos una realización.

La figura 2 representa un diagrama de bloques de un dispositivo de comunicación, de acuerdo con al menos una realización.

La figura 3 representa un diagrama de bloques de un punto final local, de acuerdo con al menos una realización.

La figura 4 representa un diagrama de flujo de un método, de acuerdo con al menos una realización.

La figura 5 representa datos de control de sesión de medios, de acuerdo con al menos una realización.

La figura 6 representa datos de transporte de sesión de medios, de acuerdo con al menos una realización.

Descripción detallada

La figura 1 representa un sistema de comunicación, de acuerdo con al menos una realización. Como se muestra, un sistema 100 de comunicación incluye un dispositivo 102 de comunicación, un punto final 104 local y un punto final 106 remoto.

El dispositivo 102 de comunicación podría adoptar la forma de, por ejemplo, un ordenador personal, un ordenador de escritorio, una laptop, un ordenador portátil, una tableta, un ordenador de mano, un ordenador de usuario, un asistente digital personal (PDA), un teléfono de funciones, un visualizador óptico montado en la cabeza (OHMD) y/o un reloj

inteligente, entre muchas otras posibilidades que conocerán los expertos en la técnica. En la realización ilustrada en la figura 1, el dispositivo 102 de comunicación toma la forma de un teléfono inteligente.

El punto final 104 local podría tomar la forma de un auricular (tal como un auricular Bluetooth), un accesorio montado en un dispositivo de comunicación (tal como un estuche o funda) y/o cualquier otra entidad capaz de llevar a cabo las funciones de punto final local descritas en este documento.

Como se muestra en la figura 1, el dispositivo 102 de comunicación está conectado comunicativamente al punto final 104 local a través de un enlace 108 de comunicación de red de área personal (PAN). En una realización, el enlace de comunicación PAN toma la forma de un enlace de comunicación Bluetooth, aunque el enlace también podría adoptar otras formas.

El punto final 106 remoto puede ser cualquier dispositivo adecuado (o combinación de dispositivos) configurado para realizar las funciones de punto final remoto descritas en este documento. En la realización ilustrada en la figura 1, el punto final 106 remoto toma la forma de un dispositivo 118 de comunicación de punto final remoto y un accesorio 116 de punto final remoto que están conectados comunicativamente a través de un enlace 120 de comunicación. El accesorio 116, el dispositivo 118 y el enlace 120 de comunicación pueden ser similares en función y/o estructura al punto final 104 local, el dispositivo 102 de comunicación y el enlace 108 de comunicación de la red de área personal (PAN) (respectivamente), como ejemplos. En otras configuraciones, el punto final 106 remoto podría tomar la forma de un teléfono criptográfico, una central secundaria privada (PBX), un PBX con protocolo de Internet (IP-PBX) y/o cualquier otra entidad capaz de llevar a cabo las funciones de punto final remoto descritas.

La figura 2 representa un diagrama de bloques de un dispositivo de comunicación, de acuerdo con al menos una realización. Como se muestra, el dispositivo 102 de comunicación incluye un procesador 202, un almacenamiento 204 de datos, una interfaz 206 de comunicación y una interfaz 208 de usuario, cada uno de los cuales está interconectado a través de un bus 210 de sistema. En la realización ilustrada en la figura 1, el punto final 106 remoto adopta la forma de un teléfono de escritorio criptográfico. Aquellos que tengan experiencia en la técnica relevante apreciarán que el dispositivo 102 de comunicación podría tener componentes adicionales y/o diferentes, y quizás una disposición diferente de componentes, entre muchas otras posibles variaciones que podrían enumerarse aquí.

El procesador 202 puede incluir uno o más procesadores de cualquier tipo que los expertos en la técnica consideren adecuados, algunos ejemplos incluyen un microprocesador, un circuito integrado de aplicación específica (ASIC) y un procesador de señal digital (DSP).

El almacenamiento 204 de datos puede tomar la forma de cualquier medio legible por ordenador no transitorio o combinación de tales medios, algunos ejemplos incluyen memoria flash, memoria de solo lectura (ROM) y memoria de acceso aleatorio (RAM) para nombrar solo unos pocos, ya que podrían usarse uno o más tipos de tecnología de almacenamiento de datos no transitorios que los expertos en la técnica consideren adecuados.

Como se presenta en la figura 2, el almacenamiento 204 de datos contiene instrucciones 210 de programa ejecutables por el procesador 202 para llevar a cabo diversas funciones, aunque el almacenamiento 204 de datos puede contener datos diferentes y/o adicionales. En una realización en la que el dispositivo 102 de comunicación está configurado para llevar a cabo uno o más procesos y/o funciones (tales como los procesos y funciones descritos con referencia a la figura 1), las instrucciones 210 de programa son ejecutables por el procesador 202 para llevar a cabo esas funciones. En los casos en los que otras entidades descritas en este documento tienen una estructura similar a la del dispositivo 102 de comunicación como se describe en relación con al menos la figura 3, las respectivas instrucciones 210 de programa almacenadas por los respectivos almacenamientos 204 de datos de esos respectivos dispositivos son ejecutables por sus respectivos procesadores 202 para llevar a cabo funciones realizadas por esos dispositivos.

La interfaz 206 de comunicación puede incluir cualquier hardware necesario (por ejemplo, conjuntos de chips, antenas, tarjetas Ethernet, etc.) y/o software para realizar una o más formas de comunicación con uno o más componentes y/o entidades (tales como el punto final 204 local y el punto final 206 remoto, como ejemplos). La interfaz 206 de comunicación puede configurarse para comunicarse de acuerdo con uno o más protocolos tales como Bluetooth, NFC, asociación de datos infrarrojos (IrDA), ZigBee, Wi-Fi, bus de serie universal (USB), IEEE 1394 (FireWire) y/o IEEE 802.3 (Ethernet)), como ejemplos.

La interfaz 208 de usuario puede incluir uno o más visualizadores, pantallas táctiles, altavoces, micrófonos, teclas de marcación, botones, conmutadores, diodos emisores de luz (LED), y similares. Uno o más componentes de interfaz de usuario (por ejemplo, un componente de pantalla táctil y visualizador interactivos) podrían proporcionar funcionalidad tanto de entrada de usuario como de salida de usuario. Y podrían implementarse otros componentes de la interfaz de usuario en un contexto dado, como conocen los expertos en la técnica.

La figura 3 representa un diagrama de bloques de un punto final local, de acuerdo con al menos una realización. Como se muestra, el punto final 104 local incluye un procesador 302, almacenamiento 304 de datos, una interfaz 306 de comunicación PAN, una interfaz 308 de usuario y un módulo 310 criptográfico, cada uno de los cuales está interconectado a través de un bus 312 de sistema. Aquellos que tienen experiencia en la técnica relevante apreciará que el punto final 104 local podría tener componentes adicionales y/o diferentes, y quizás una disposición diferente de componentes, entre muchas otras variaciones posibles que podrían enumerarse aquí. El procesador 302, el

almacenamiento 304 de datos, la interfaz 306 de comunicación PAN y/o la interfaz 308 de usuario pueden funcionar de una manera similar a las entidades de nombre similar del dispositivo 102 de comunicación, como se describe (por ejemplo) con respecto a la figura 2 anterior.

El módulo 310 criptográfico puede incluir hardware y/o software para realizar funciones o procesos criptográficos, por ejemplo, encriptado, desencriptado, generación de firmas, verificación de firmas y/o generación de claves. En una realización, el módulo 310 criptográfico está contenido dentro de un perímetro definido explícitamente que establece los límites físicos del módulo criptográfico y que contiene procesadores y/u otros componentes de hardware que almacenan y protegen cualquier componente de software y firmware del módulo criptográfico. El módulo 310 criptográfico podría tomar la forma de (o incluir) un criptoprocesador seguro, una tarjeta inteligente, una tarjeta digital segura (SD), una tarjeta micro SD, una tarjeta de módulo de identidad de suscriptor (SIM) y/o cualquier otro módulo criptográfico, conocido por un experto en la técnica.

La figura 4 representa un diagrama de flujo de un método, de acuerdo con al menos una realización. Como se muestra, el método 400 comienza en el paso 402 con el dispositivo 102 de comunicación recibiendo una solicitud para establecer una sesión de medios con el punto final 106 remoto. La sesión de medios podría tomar la forma de (o incluir) una llamada telefónica y/o una vídeoconferencia, entre otras posibilidades.

El dispositivo 102 de comunicación puede recibir la solicitud a través de la interfaz 208 de usuario. Por ejemplo, el dispositivo 102 de comunicación puede recibir la solicitud como resultado de que un usuario navegue por un conjunto de uno o más contactos a través de la interfaz 208 de usuario y luego seleccione un contacto (o quizás múltiples contactos) con quienes el usuario quisiera establecer una sesión de medios.

Adicional o alternativamente, el dispositivo 102 de comunicación puede recibir la solicitud desde el punto final 104 local. Por ejemplo, el dispositivo 102 de comunicación puede recibir la solicitud como una señal de audio que representa un comando hablado tal como "llamar a John". Como otro ejemplo, el dispositivo 102 de comunicación podría recibir la solicitud como un comando de Bluetooth que indique al dispositivo 102 de comunicación que establezca una sesión de medios con un contacto dado (por ejemplo, un contacto resaltado a través de la interfaz 208 de usuario del dispositivo 102 de comunicación).

Como otra posibilidad, el dispositivo 102 de comunicación puede recibir la solicitud desde el punto final 106 remoto. La solicitud podría tomar la forma de un mensaje de origen de llamada, un mensaje de protocolo de inicio de sesión (SIP), un protocolo de transporte en tiempo real (RTP) mensaje, un mensaje RTP seguro (SRTP), un mensaje ZRTP, un mensaje de protocolo de descripción de sesión (SDP), un mensaje H.323, un mensaje de intercambio inter-asteriscos (IAX) y/o un mensaje IAX2, entre muchas otras posibilidades eso será evidente para los expertos en la técnica.

Los expertos en la técnica apreciarán que el dispositivo 102 de comunicación también puede recibir la solicitud de otras formas, incluyendo cualquier combinación de los ejemplos proporcionados anteriormente. Por ejemplo, el dispositivo 102 de comunicación podría recibir un mensaje SIP desde el punto final 104 local a través de una conexión Bluetooth. La solicitud también podría adoptar otras formas.

En el paso 404, el dispositivo 102 de comunicación, en respuesta a la recepción de la solicitud, intercambia datos de control de sesión de medios con el punto final 106 remoto en nombre del punto final 104 local para establecer la sesión de medios solicitada entre el punto final 104 local y el punto final 106 remoto. El intercambio de datos de control de la sesión de medios podría incluir recibir los datos de control de la sesión de medios desde el punto final 106 remoto y/o enviar los datos de control de la sesión de medios al punto final 106 remoto, como ejemplos. Los datos de control de la sesión de medios pueden tomar la forma de (o incluir) datos SIP, datos RTP, datos SRTP, datos ZRTP, datos SDP, datos H.323, datos IAX y/o datos IAX2, entre muchas otras posibilidades que resultarán evidentes para los expertos en la técnica.

La figura 5 representa datos de control de sesión de medios, de acuerdo con al menos una realización. Como se muestra, los datos 500 de control de sesión de medios incluyen metadatos 502, una clave 504 criptográfica y una firma 506 digital.

En al menos una realización, los metadatos 502 toman la forma de (o incluyen) metadatos asociados con la sesión de medios solicitada. Por ejemplo, si el dispositivo 102 de comunicación recibe la solicitud del punto final 106 remoto como un mensaje SIP que incluye un identificador de mensaje SIP, entonces los metadatos 502 podrían incluir el identificador de mensaje SIP. Como otro ejemplo, los metadatos 502 podrían incluir un identificador de origen y/o un identificador de destino tal como un número de teléfono, una dirección de protocolo de Internet (IP) y/o un identificador uniforme de recursos (URI). Los metadatos 502 también podrían adoptar otras formas.

La clave 504 criptográfica podría tomar la forma de (o incluir) una clave pública que está asociada con una clave privada. Las claves públicas y/o privadas podrían adoptar la forma de claves RSA respectivas, entre otras posibilidades que conocerán los expertos en la técnica. Tanto la clave privada como la clave pública, o ambas, pueden estar asociadas con el punto final 106 remoto. Por ejemplo, el punto final 106 remoto puede haber generado tanto la clave pública como la clave privada. Como otro ejemplo, el punto final 106 remoto puede almacenar la clave privada, por ejemplo, en un módulo criptográfico similar al módulo 310 criptográfico.

En lugar de (o además de) la clave 504 criptográfica, los datos 500 de control de sesión de medios podrían incluir datos de intercambio de clave de sesión de medios. Los datos de intercambio de clave podrían tomar la forma de (o incluir) componentes de un intercambio de claves Diffie-Hellman, que podrían ser utilizados por el punto final 104 local y/o el punto final 106 remoto para establecer una clave criptográfica compartida. Los datos de intercambio de clave también podrían adoptar otras formas.

La firma 506 digital podría tomar la forma de (o incluir) una firma digital generada por el punto final 106 remoto con base en una clave privada que está asociada con el punto final remoto. Por ejemplo, la firma digital puede ser una firma generada con base en un hash criptográfico de metadatos 502 (y/u otros datos en los datos 500 de control de sesión de medios) y además con base en una clave privada almacenada en un módulo criptográfico del punto final 106 remoto. La clave privada podría almacenarse además en el módulo 310 criptográfico del punto final 104 local (por ejemplo, si la firma 506 digital toma la forma de un código de autenticación de mensaje).

Adicional o alternativamente, la firma 506 digital podría tomar la forma de (o incluir) una firma digital generada por un tercero de confianza, tal como una autoridad de certificación centralizada y/o una parte de firma de clave descentralizada (por ejemplo, como como en un modelo de autenticación de web de confianza). En una realización en la que los datos 500 de control de sesión de medios incluyen tanto la clave 504 criptográfica como la firma 506 digital, la firma digital puede basarse en la clave criptográfica y puede ser generada por el tercero de confianza con base en la clave criptográfica.

Los expertos en la técnica entenderán que los datos 500 de control de sesión de medios pueden incluir datos diferentes y/o adicionales. Por ejemplo, en algunas realizaciones, los datos 502 de control de sesión de medios pueden no incluir la clave 504 criptográfica o la firma 506 digital. También son posibles otras variaciones.

En el paso 406, el dispositivo 102 de comunicación retransmite datos de la carga útil de la sesión de medios entre el punto final 104 local y el punto final 106 remoto. Los datos de la carga útil de la sesión de medios se asocian con la sesión de medios y (ii) se encriptan con base en al menos una clave criptográfica de datos de carga útil que no es accesible para el dispositivo 102 de comunicación. En una realización, la clave criptográfica de datos de carga útil toma la forma de una clave almacenada en el módulo 310 criptográfico del punto final 104 local, y podría ser una clave simétrica (quizás establecida mediante un intercambio de claves Diffie-Hellman entre el punto final 104 local y el punto final 106 remoto) y/o una clave privada que es parte de un par de claves asimétricas, como ejemplos. En otra realización, la clave criptográfica de datos de carga útil toma la forma de una clave almacenada en un módulo criptográfico del punto final 106 remoto y podría ser una clave simétrica y/o una clave pública que está asociada con una clave privada (por ejemplo, una clave privada almacenada en el módulo 310 criptográfico del punto final 104 local).

En una realización, la retransmisión de los datos de carga útil de la sesión de medios incluye la retransmisión de datos de transporte de la sesión de medios que incluyen los datos de la carga útil de la sesión de medios, posiblemente además de otros datos.

La figura 6 representa datos de transporte de sesión de medios, de acuerdo con al menos una realización. Como se muestra en la figura 6, los datos 600 de transporte de sesión de medios incluyen metadatos 602 de sesión de medios, datos 604 de carga útil de la sesión de medios, metadatos 606 de datos de carga útil, y una firma 608 digital.

Los metadatos 602 de la sesión de medios podrían tomar la forma de (o incluir) metadatos asociados con la sesión de medios solicitada. En algunas realizaciones, los metadatos de la sesión de medios toman una forma similar a la de los metadatos 502 asociados con la sesión de medios solicitada. En una realización, los metadatos 602 de sesión de medios identifican los datos 604 de carga útil de la sesión de medios como asociados con la sesión de medios.

Los metadatos 606 de datos de carga útil podrían tomar la forma de (o incluir) metadatos asociados con datos 604 de carga útil de la sesión de medios. Por ejemplo, los metadatos 606 podrían identificar una clave criptográfica determinada que se utilizó para encriptar los datos 604 de carga útil de la sesión de medios y/o que puede usarse para desencriptar datos 604 de carga útil de la sesión de medios. Los metadatos 606 podrían identificar un códec (por ejemplo, un códec de audio y/o un códec de vídeo) usado para codificar los medios representados por datos 604 de carga útil de la sesión de medios. Los metadatos 606 podría incluir datos de temporización y/o datos de pedido para las respectivas cargas útiles de sesión de medios de datos, tales como datos 604 de carga útil de la sesión de medios. Los metadatos 606 también podrían adoptar otras formas.

La firma 608 digital puede basarse en datos 604 de carga útil de la sesión de medios. Para simplificar la generación y verificación de la firma 608 digital, la firma digital puede basarse en un hash (por ejemplo, un hash criptográfico) de los datos de carga útil de sesión de medios. El hash se puede generar usando una función hash tal como SHA-1 y/o MD5, como ejemplos. La firma 608 digital puede ser generada por el punto final 106 remoto con base en los datos 604 de carga útil de la sesión de medios.

La retransmisión de datos 604 de carga útil de la sesión de medios puede incluir retransmitir los datos de carga útil de sesión de medios entre el dispositivo 102 de comunicación y el punto final 104 local a través del enlace 108 de comunicación PAN. En una realización, el enlace 108 de comunicación PAN toma la forma de un enlace de comunicación Bluetooth, y retransmitir datos 604 de carga útil de la sesión de medios entre el dispositivo 102 de

comunicación y el punto final 104 local a través del enlace de comunicación PAN toma la forma de (o incluye) retransmitir los datos de carga útil de sesión de medios a través del enlace de comunicación Bluetooth.

La retransmisión de datos 604 de carga útil de la sesión de medios a través del enlace de comunicación Bluetooth puede incluir retransmitir los datos de carga útil de sesión de medios de acuerdo con un primer perfil de Bluetooth. El primer perfil de Bluetooth podría tomar la forma de (o incluir) un perfil de distribución de audio avanzado (A2DP) y/o un perfil de audio de Bluetooth, como ejemplos. Los datos 604 de carga útil de la sesión de medios pueden pasarse al punto final 104 local a través del perfil de audio de Bluetooth sin que el dispositivo 102 de comunicación altere los datos de la carga útil de la sesión de medios. Al retransmitir los datos de carga útil de la sesión de medios de acuerdo con un perfil de audio de Bluetooth, las modificaciones a un Bluetooth genérico para permitir una comunicación segura pueden ser mínimas.

El dispositivo 102 de comunicación puede proporcionar datos de control de sesión de medios de punto final local al punto final 104 local a través del enlace de comunicación PAN. El control de sesión de medios de punto final local puede basarse en los datos de control de sesión de medios, por ejemplo, y podría incluir una clave criptográfica (por ejemplo, una clave pública), una firma digital (por ejemplo, de una clave criptográfica y/o de datos de carga útil de sesión de medios), metadatos de sesión de medios y/o metadatos de datos de carga útil, entre otras posibilidades. Dichos datos de control de sesión de medios de punto final local pueden ser utilizados por el punto final 104 local para encriptar y/o desencriptar datos 608 de carga útil de sesión de medios, por ejemplo.

En una realización, el enlace 108 de comunicación PAN toma la forma de un enlace de comunicación Bluetooth y el suministro de datos de control de la sesión de medios del punto final local al punto final 104 local a través del enlace de comunicación PAN toma la forma de proporcionar los datos de control de la sesión de medios del punto final local a través del enlace de comunicación Bluetooth. Proporcionar los datos de control de la sesión de medios del punto final local a través del enlace de comunicación Bluetooth podría incluir proporcionar los datos de control de la sesión de medios del punto final local de acuerdo con un segundo perfil de Bluetooth que es diferente del primer perfil de Bluetooth. El segundo perfil de Bluetooth podría tomar la forma de (o incluir) un perfil de puerto serial (SPP) y/o un perfil de Bluetooth sin audio, como ejemplos.

REIVINDICACIONES

1. Un método que comprende:

un dispositivo de comunicación que recibe una solicitud para establecer una sesión de medios con un punto final remoto;

En respuesta a la recepción de la solicitud, el dispositivo de comunicación intercambia datos de control de sesión de medios con el punto final remoto en nombre de un punto final local para establecer la sesión de medios solicitada entre el punto final local y el punto final remoto, en donde el dispositivo de comunicación está conectado comunicativamente al punto final local a través de un enlace de comunicación de red de área personal (PAN), el enlace de comunicación PAN comprende un enlace de comunicación Bluetooth; y

el dispositivo de comunicación que retransmite datos de la carga útil de la sesión de medios entre los puntos finales locales y remotos, en donde los datos de la carga útil de la sesión de medios (i) están asociados con la sesión de medios y (ii) están encriptados con base en al menos una clave criptográfica de datos de la carga útil que es no accesible al dispositivo de comunicación,

caracterizado porque la retransmisión de los datos de la carga útil de la sesión de medios comprende la retransmisión de los datos de la carga útil de la sesión de medios a través del enlace de comunicación Bluetooth de acuerdo con un primer perfil de Bluetooth que incluye un perfil de distribución de audio avanzado (A2DP),

y porque el dispositivo de comunicación proporciona datos de control de sesión de medios de punto final local al punto final local a través del enlace de comunicación Bluetooth de acuerdo con un segundo perfil de Bluetooth que es diferente del primer perfil de Bluetooth, el segundo perfil de Bluetooth incluye un perfil de puerto serial (SPP) o un perfil de Bluetooth sin audio, los datos de control de la sesión de medios de punto final local se basan en los datos de control de la sesión de medios.

2. El método de la reivindicación 1, en donde los datos de control de la sesión de medios comprenden metadatos asociados con la sesión de medios.

3. El método de cualquiera de las reivindicaciones 1-2, en donde los datos de control de la sesión de medios comprenden una segunda clave criptográfica.

4. El método de la reivindicación 3, en donde la segunda clave criptográfica comprende una clave pública que está asociada con una clave privada, en donde la clave privada está asociada con el punto final remoto.

5. El método de la reivindicación 3, en donde la clave criptográfica de datos de carga útil se basa en la segunda clave criptográfica.

6. El método de cualquiera de las reivindicaciones 1-5, en donde los datos de control de la sesión de medios comprenden datos de intercambio de clave de la sesión de medios.

7. El método de cualquiera de las reivindicaciones 1-6, en donde los datos de control de la sesión de medios comprenden una firma digital.

8. El método de la reivindicación 7, en donde la firma digital comprende una firma digital generada por el punto final remoto con base en una clave privada que está asociada con el punto final remoto.

9. El método de cualquiera de las reivindicaciones 7-8, en donde la firma digital comprende una firma digital generada por un tercero de confianza.

10. El método de cualquiera de las reivindicaciones 7-9, en donde:

los datos de control de sesión de medios recibidos comprenden además una segunda clave criptográfica; y

la firma digital se basa en la segunda clave criptográfica.

11. El método de cualquiera de las reivindicaciones 1-10, en donde los datos de control de la sesión de medios comprenden uno o más de (i) datos del protocolo inicial de sesión (SIP), (ii) datos ZRTP, (iii)) datos del protocolo de transporte seguro en tiempo real (SRTP) y (iv) datos de protocolo de descripción de sesión (SDP).

12. El método de cualquiera de las reivindicaciones 1-11, en donde:

retransmitir los datos de la carga útil de la sesión de medios comprende retransmitir los datos de la carga útil de la sesión de medios que incluyen tanto los datos de la carga útil de la sesión de medios como una firma digital que se basa en los datos de la carga útil de la sesión de medios; y

la firma digital comprende una firma digital generada por el punto final remoto con base en los datos de carga útil de la sesión de medios.

13. Un dispositivo de comunicación que comprende:

una interfaz de comunicación;

un procesador; y almacenamiento de datos que contiene instrucciones ejecutables por el procesador para hacer que el dispositivo de comunicación lleve a cabo un conjunto de funciones, el conjunto de funciones que comprende:

un dispositivo de comunicación que recibe una solicitud para establecer una sesión de medios con un punto final remoto;

en respuesta a la recepción de la solicitud, el dispositivo de comunicación intercambia datos de control de sesión de medios con el punto final remoto en nombre de un punto final local para establecer la sesión de medios solicitada entre el punto final local y el punto final remoto, en donde el dispositivo de comunicación está conectado comunicativamente al punto final local a través de un enlace de comunicación de red de área personal (PAN), el enlace de comunicación PAN comprende un enlace de comunicación Bluetooth; y

el dispositivo de comunicación que retransmite datos de la carga útil de la sesión de medios entre los puntos finales locales y remotos, en donde los datos de la carga útil de la sesión de medios (i) están asociados con la sesión de medios y (ii) están encriptados con base en al menos una clave criptográfica de datos de la carga útil que es no accesible al dispositivo de comunicación,

caracterizado porque la retransmisión de los datos de la carga útil de la sesión de medios comprende la retransmisión de los datos de la carga útil de la sesión de medios a través del enlace de comunicación Bluetooth de acuerdo con un primer perfil de Bluetooth que incluye un perfil de distribución de audio avanzado (A2DP),

y porque el dispositivo de comunicación proporciona datos de control de sesión de medios de punto final local al punto final local a través del enlace de comunicación Bluetooth de acuerdo con un segundo perfil de Bluetooth que es diferente del primer perfil de Bluetooth, el segundo perfil de Bluetooth incluye un perfil de puerto serial (SPP) o un perfil de Bluetooth sin audio, los datos de control de la sesión de medios de punto final local se basan en los datos de control de la sesión de medios.

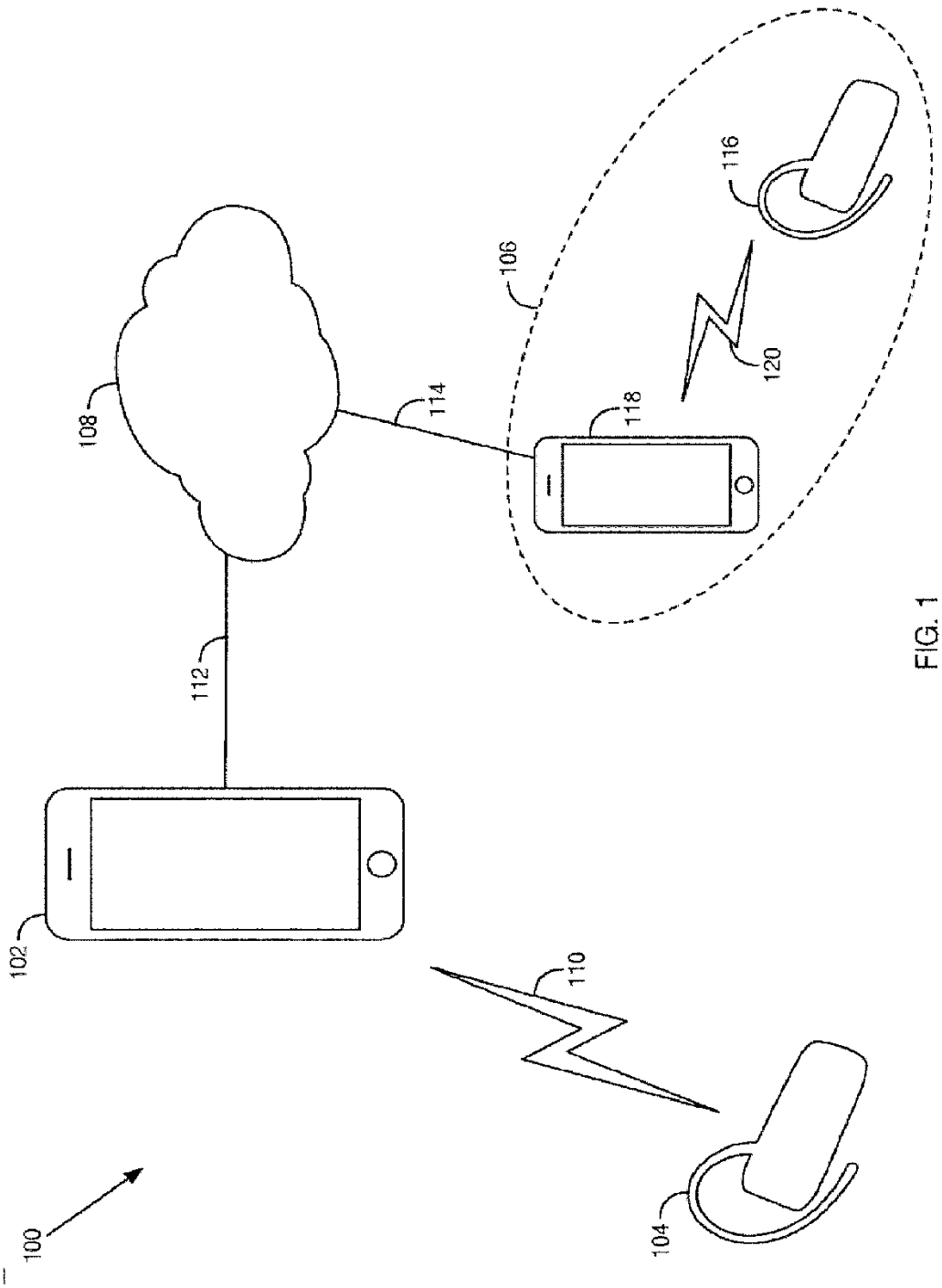

FIG. 1

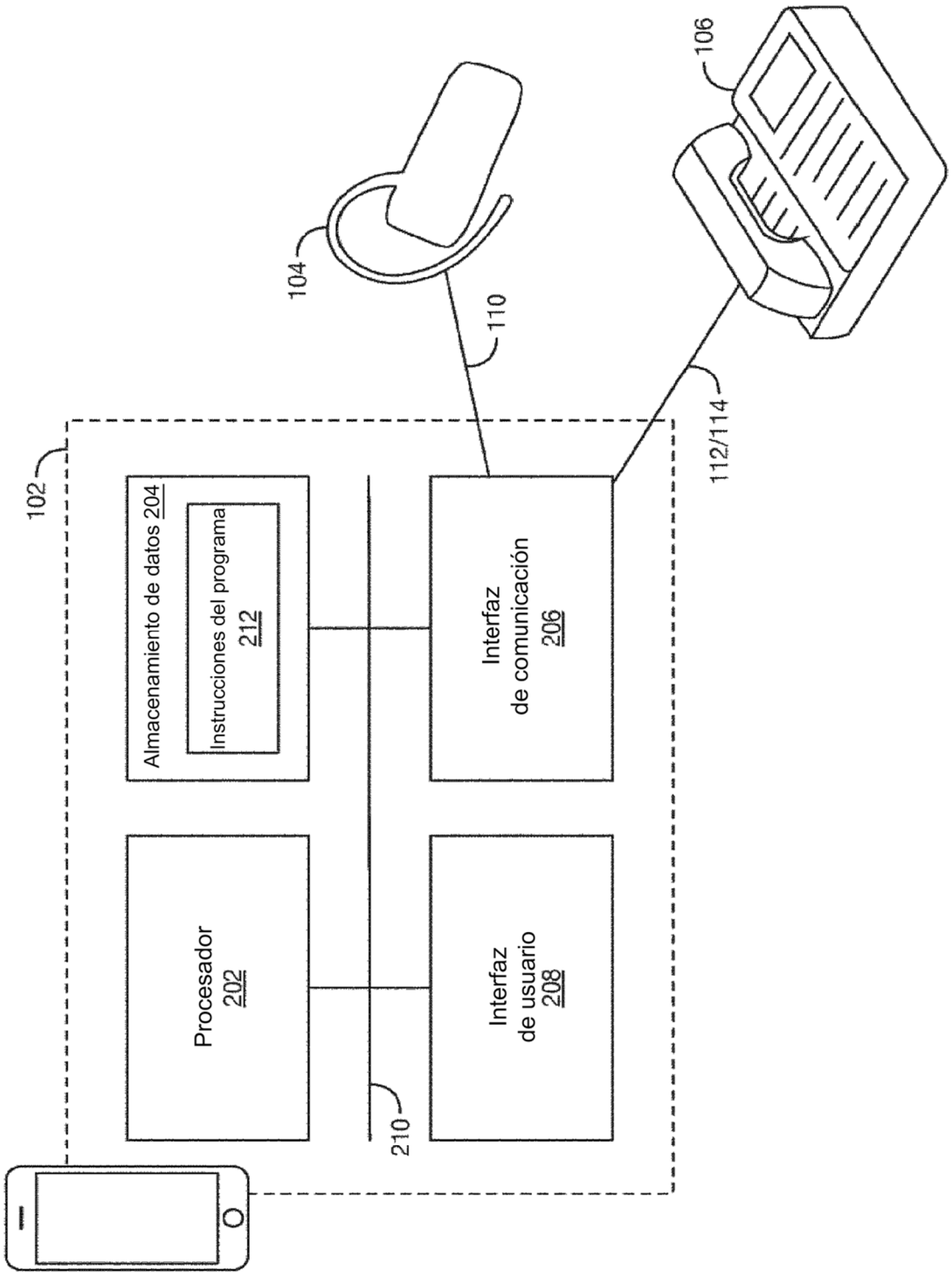
102
Almacenamiento de datos 204
Instrucciones del programa 212
Procesador 202
Interfaz de comunicación 206
Interfaz de usuario 208
210
104
110
106
112/114

FIG. 2

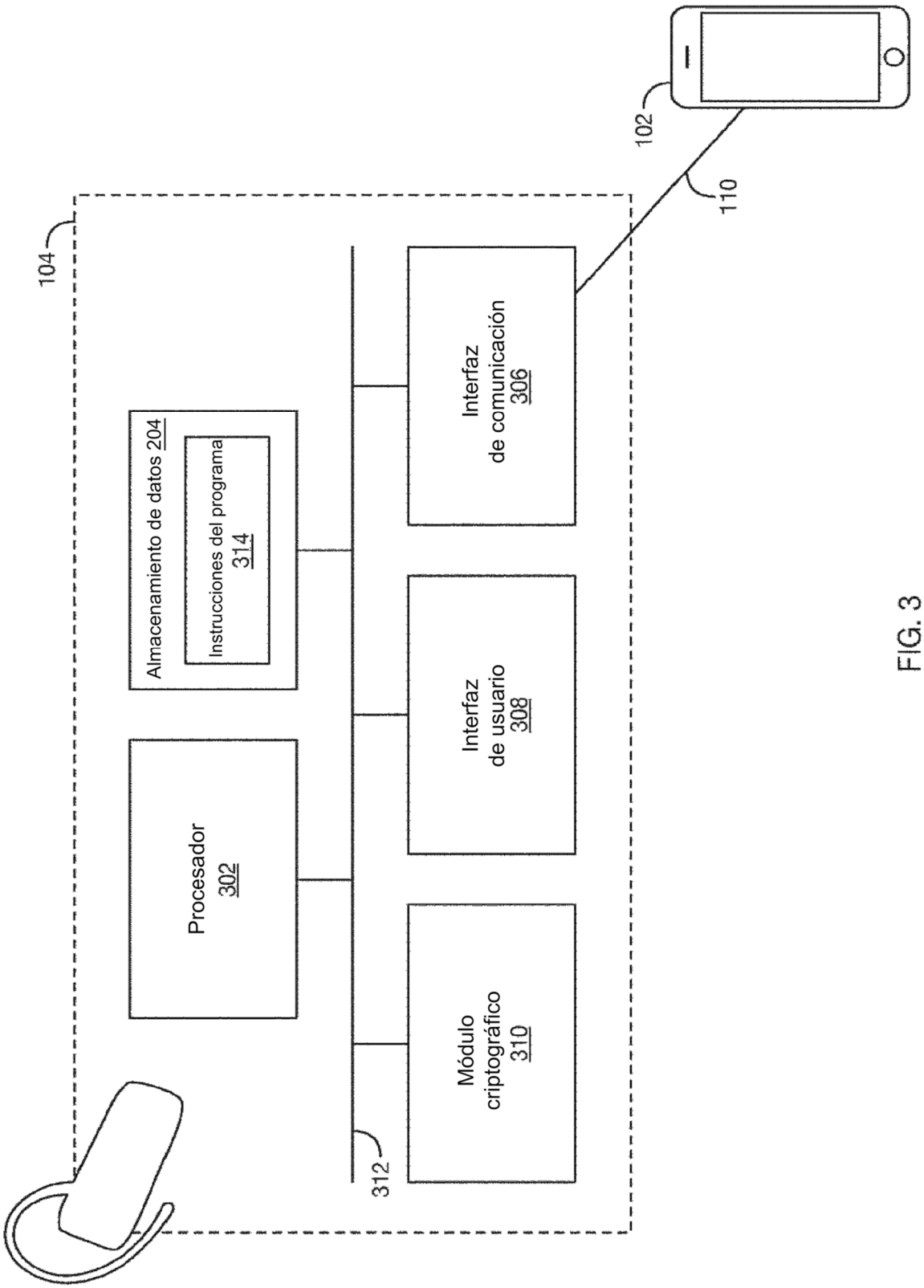
102
110
104
Interfaz de comunicación 306
Almacenamiento de datos 204
Instrucciones del programa 314
Interfaz de usuario 308
Procesador 302
Módulo criptográfico 310
312

FIG. 3

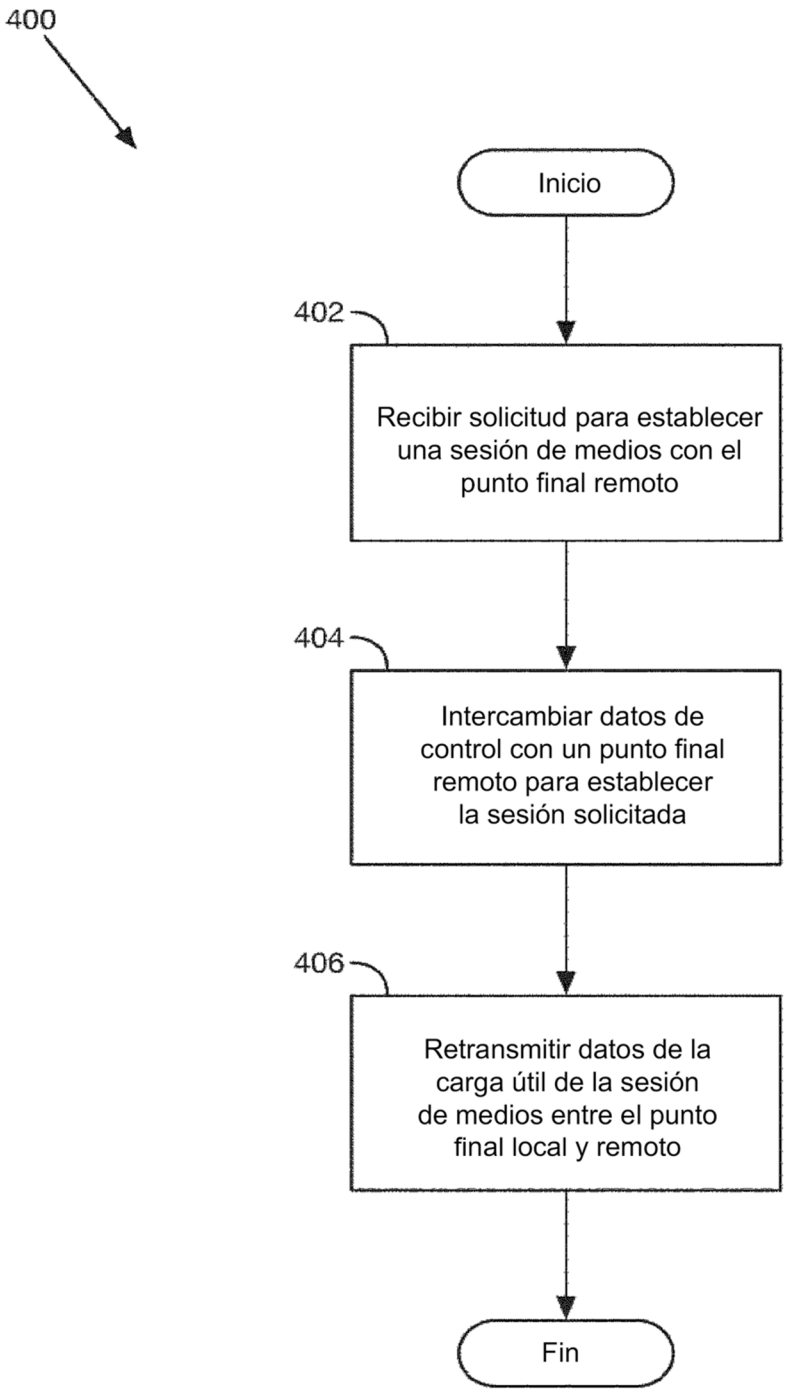
400
Inicio
402
Recibir solicitud para establecer una sesión de medios con el punto final remoto
404
Intercambiar datos de control con un punto final remoto para establecer la sesión solicitada
406
Retransmitir datos de la carga útil de la sesión de medios entre el punto final local y remoto
Fin

FIG. 4

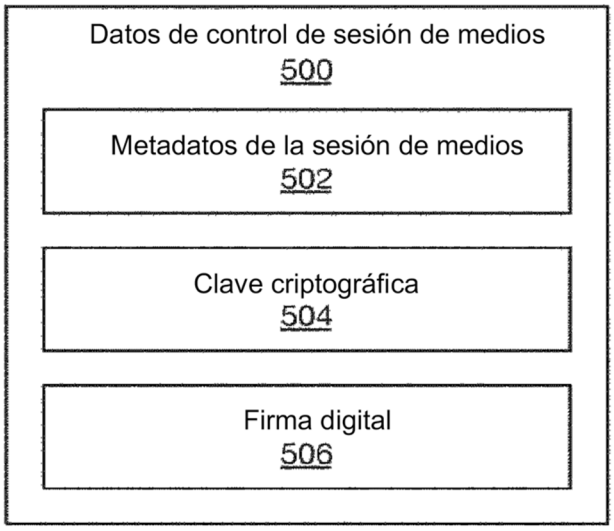
Datos de control de sesión de medios
500
Metadatos de la sesión de medios
502
Clave criptográfica
504
Firma digital
506

FIG. 5

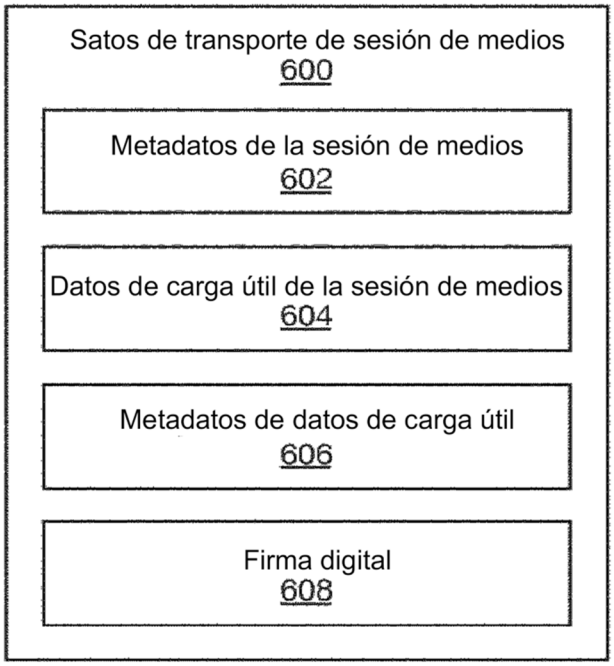
Satos de transporte de sesión de medios
600
Metadatos de la sesión de medios
602
Datos de carga útil de la sesión de medios
604
Metadatos de datos de carga útil
606
Firma digital
608

FIG. 6