(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 954 499**

(51) Int. CI.:

H04L 9/40 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **31.10.2019 E 19206500 (1)**

(97) Fecha y número de publicación de la concesión europea: **09.08.2023 EP 3651431**

(54) Título: **Métodos y dispositivos para establecer canales de comunicación seguros**

(30) Prioridad:

06.11.2018 US 201816181755

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.11.2023

(73) Titular/es:

MALIKIE INNOVATIONS LIMITED (100.0%)
The Glasshouses GH2, 92 Georges Street Lower
Dun Laoghaire, Dublin A96 VR66, IE

(72) Inventor/es:

YANG, CHANG FUNG y
XU, JASON SONGBO

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Métodos y dispositivos para establecer canales de comunicación seguros

Campo

La presente solicitud se refiere en general a las comunicaciones en red y, en particular, a métodos y sistemas para establecer un canal de comunicación seguro entre dispositivos de comunicación.

Antecedentes

Un dispositivo de comunicación puede comunicarse con otro dispositivo de comunicación a través de una red a través de un canal de comunicación seguro. Los respectivos dispositivos de comunicación pueden negociar qué algoritmos usar para preparar los datos para la transmisión por el canal de comunicación seguro. Por ejemplo, las opciones de algoritmos negociados pueden incluir algoritmos de cifrado o integridad para usar al preparar los datos para el intercambio a través del canal de comunicación seguro. Los dispositivos de comunicación también pueden negociar el nivel de seguridad de las claves de cifrado o la función pseudoaleatoria que se usará al preparar los datos. La negociación a menudo se realiza antes del intercambio de datos y si un conjunto de opciones de algoritmo soportadas por un dispositivo de comunicación no coincide con un conjunto de opciones de algoritmo soportadas por otro dispositivo de comunicación, la comunicación segura entre esos dispositivos de comunicación puede no ser posible.

El antecedente relevante de la técnica está representado por el documento de Milutinovic Milica et al: "Secure Negotiation for Manual Authentication Protocols", Conferencia internacional sobre criptografía financiera y seguridad de datos; Documentos US 7219223 B1; EP 2007110 A1 y US 2011/078436 A1.

Compendio

La invención se define como un método, un dispositivo informático y un programa informático como se detalla en las reivindicaciones siguientes.

Breve descripción de los dibujos

Ahora se hará referencia, a modo de ejemplo, a los dibujos adjuntos que muestran ejemplos de realización de la presente solicitud, y en los que:

La FIG. 1 ilustra, en forma de diagrama de bloques, un sistema para establecer un canal de comunicación seguro entre un dispositivo de comunicación de origen y un dispositivo de comunicación de destino, de acuerdo con un ejemplo de la presente solicitud;

la FIG. 2 ilustra, en forma de diagrama de flujo, un método para establecer un canal de comunicación seguro entre el dispositivo de comunicación de origen y el dispositivo de comunicación de destino de la FIG. 1;

la FIG. 3 ilustra esquemáticamente una interfaz de usuario que incluye opciones de algoritmo seleccionables, de acuerdo con un ejemplo de la presente solicitud;

la FIG. 4 ilustra esquemáticamente una interfaz de usuario, de acuerdo con otro ejemplo de la presente solicitud; y

la FIG. 5 ilustra, en forma de diagrama de bloques simplificado, un dispositivo electrónico, de acuerdo con un ejemplo de la presente solicitud.

Es posible que se hayan usado números de referencia similares en diferentes figuras para indicar componentes similares.

Descripción de las realizaciones de ejemplo

En un primer aspecto, la presente solicitud describe un método para establecer un canal de comunicación seguro entre un primer dispositivo de comunicación y un segundo dispositivo de comunicación. El canal de comunicación seguro está definido por una o más opciones de algoritmo. La una o más opciones de algoritmo están asociadas con una de una o más categorías de opciones. El método incluye: recibir, a través de un módulo de entrada, una señal que representa una o más selecciones, estando la respectiva una o más selecciones asociadas con una de una o más categorías de opciones; para las respectivas categorías de opciones, generar una lista ordenada de opciones de algoritmos con base en las selecciones recibidas; generar una propuesta de asociación de seguridad que incluye una o más de las opciones de algoritmo de las respectivas listas ordenadas de opciones de algoritmo, en donde la propuesta de asociación de seguridad se genera con base en un orden en la lista ordenada de opciones de algoritmo; y transmitir la propuesta de asociación de seguridad al segundo dispositivo de comunicación para establecer el canal de comunicación seguro.

En otro aspecto, la presente solicitud describe un dispositivo de cálculo que comprende: un módulo de comunicaciones; un módulo de entrada; un elemento de visualización; un procesador acoplado al módulo de comunicaciones, el elemento de visualización y el módulo de entrada; y una memoria acoplada al procesador. La memoria almacena instrucciones ejecutables por el procesador para establecer un canal de comunicación seguro entre el dispositivo informático y un segundo dispositivo de comunicación. El canal de comunicación seguro está definido por una o más opciones de algoritmo y la una o más opciones de algoritmo están asociadas con una de una o más categorías de opciones. Las instrucciones ejecutables por el procesador, cuando se ejecutan, configuran el procesador para: recibir, a través del módulo de entrada, una señal que representa una o más selecciones, estando la respectiva una o más selecciones asociadas con una de las una o más categorías de opciones; para las respectivas categorías de opciones, generar una lista ordenada de opciones de algoritmos con base en las selecciones recibidas; generar una propuesta de asociación de seguridad que incluye una o más de las opciones de algoritmo de las respectivas listas ordenadas de opciones de algoritmo, en donde la propuesta de asociación de seguridad se genera con base en un orden en la lista ordenada de opciones de algoritmo; y transmitir la propuesta de asociación de seguridad al segundo dispositivo de comunicación para establecer el canal de comunicación seguro.

En otro aspecto más, la presente solicitud describe un medio de almacenamiento legible por ordenador no transitorio que almacena instrucciones legibles por procesador que, cuando se ejecutan, configuran un procesador para realizar uno o más de los métodos descritos en este documento. A este respecto, el término procesador pretende incluir todo tipo de circuitos de procesamiento o chips capaces de ejecutar instrucciones de programa.

Los expertos en la técnica comprenderán otros aspectos y características de la presente solicitud a partir de una revisión de la siguiente descripción de ejemplos junto con las figuras adjuntas.

En la presente solicitud, los términos "alrededor de", "aproximadamente" y "sustancialmente" pretenden cubrir variaciones que pueden existir en los límites superior e inferior de los rangos de valores, tales como variaciones en propiedades, parámetros y dimensiones. En un ejemplo no limitante, los términos "alrededor de", "aproximadamente" y "sustancialmente" pueden significar más o menos el 10 por ciento o menos.

En la presente solicitud, el término "y/o" pretende cubrir todas las combinaciones y subcombinaciones posibles de los elementos enumerados, incluido cualquiera de los elementos enumerados solo, cualquier subcombinación o todos los elementos, y sin excluyendo necesariamente elementos adicionales.

En la presente solicitud, la frase "al menos uno de... o.." pretende cubrir uno o más de los elementos enumerados, incluido cualquiera de los elementos enumerados solo, cualquier subcombinación o la totalidad de los elementos, sin excluir necesariamente ningún elemento adicional, y sin requerir necesariamente todos los elementos.

La tecnología de comunicación segura permite que un dispositivo de comunicación de origen transmita datos de forma segura a un dispositivo de comunicación de destino, y viceversa, mediante la preparación y transmisión de datos mediante algoritmos compatibles con los respectivos dispositivos de comunicación. Antes del intercambio de datos, el dispositivo de comunicación de origen negocia con el dispositivo de comunicación de destino las opciones de algoritmo que se van a usar. En algunos ejemplos, las opciones de algoritmos pueden incluir, por ejemplo, grupos Diffie-Hellman (grupos DH), algoritmos de cifrado, algoritmos de integridad o algoritmos de funciones pseudoaleatorias.

En algunos ejemplos, los protocolos de Intercambio de Claves de Internet (IKE)/Seguridad de Protocolo de Internet (IPSec) pueden usar grupos DH, como los grupos de Intercambio de Claves de Internet Versión 2 (IKEv2). La Autoridad de Números Asignados de Internet (IANA) puede definir ejemplos de grupos IKEv2 (consulte, por ejemplo, https://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml#ikev2-parameters-8). Para facilitar la exposición, en algunos ejemplos descritos en este documento, la configuración del grupo DH puede incluir los números 20, 19, 15, 1 de grupo o ninguno. Puede apreciarse que algunos protocolos pueden no utilizar grupos DH o similares como opciones de algoritmo, y en estos otros protocolos, los grupos DH no son opciones de algoritmo seleccionables.

Un algoritmo de cifrado puede definir el tipo de algoritmo que se usará para cifrar datos para su transmisión a través de un canal de comunicación. Los algoritmos de cifrado de ejemplo pueden incluir algoritmos Galois Estándar de Cifrado Avanzado/de Modo Contador (AES-GCM), como AES-GCM-256 o AES-GCM-128, algoritmos de Encadenamiento Bloqueador de Cifrado Estándar de Encriptación Avanzada (AES-CBC), como AES-CBC-256 o AES-CBC-128, Chacha20 o sin cifrado. Un algoritmo de integridad puede definir el tipo de algoritmo que se usará para verificar que los datos transmitidos a través del canal de comunicación no hayan sido manipulados o comprometidos. Los algoritmos de integridad de ejemplo pueden incluir algoritmos Hash Seguros de Código de Autenticación de Mensajes basados en Hash (HMAC-SHA), como HMAC-SHA-512-256, HMAC-SHA-384-192, HMAC-SHA-256-128, HMAC-SHA-1-96, algoritmos AES-GCM, como AES-GCM-128 o AES-GCM-256, o algoritmos Poly 1305. En algunos ejemplos, el algoritmo de cifrado ChaCha20 y el algoritmo de integridad Poly1305 se pueden usar juntos (por ejemplo, un modo "combinado" ChaCha20-Poly1305). La combinación de opciones del algoritmo ChaCha20-Poly1305 se describe, por ejemplo, por el Grupo de Trabajo de Investigación de Internet (IRTF) (consulte, por ejemplo, https://tools.ietf.org/html/rfc7539).

Una función pseudoaleatoria es una función computable para proporcionar una salida en respuesta a una entrada recibida. Las funciones pseudoaleatorias de ejemplo pueden incluir HMAC-SHA-512, HMAC-SHA-384, HMAC-SHA-256 o HMAC-SHA-1. Los grupos DH, los algoritmos de cifrado, los algoritmos de integridad y las funciones pseudoaleatorias son categorías de opciones de ejemplo. Aunque se describen cuatro categorías de opciones diferentes, se contemplan otras categorías de opciones para definir opciones de algoritmos relevantes para establecer un canal de comunicación seguro entre dispositivos de comunicación. Además, para algunos protocolos para establecer un canal de comunicación seguro, una o más de las categorías de opciones de algoritmos pueden no ser relevantes.

Como se ha descrito, antes del intercambio seguro de datos entre los dispositivos de comunicación, los respectivos dispositivos de comunicación pueden negociar las opciones de algoritmo que se usarán para preparar los datos para la transmisión por el canal de comunicación seguro. Antes del proceso de negociación, un dispositivo de comunicación de origen puede determinar la combinación de opciones de algoritmo que se propondrá a un dispositivo de comunicación de destino. En algunas implementaciones, las propuestas de algoritmos pueden ser un conjunto preseleccionado. Por ejemplo, en el protocolo Seguridad de Capa de Transporte (TLS), un conjunto preseleccionado de opciones/configuraciones de algoritmo se codifica con identificadores. Por ejemplo, un conjunto de cifrado identificado como TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 puede asociarse con un conjunto preseleccionado de configuraciones (por ejemplo, intercambio de claves de curva elíptica diffie-hellman (ECDHE), algoritmo de firma digital de curva elíptica (ECDSA), cifrado AES-256-GCM y autenticación SHA384). En la presente implementación de ejemplo, si el dispositivo de comunicación de destino no puede soportar al menos una de las opciones de algoritmo preseleccionadas, la propuesta de algoritmo completa se considerará inutilizable. Como puede que no haya forma de separar las configuraciones individuales de la propuesta de algoritmo, el dispositivo de comunicación de destino solo puede evaluar las propuestas de algoritmo respectivas como un conjunto discreto preseleccionado de opciones de algoritmo en lugar de poder elegir configuraciones de algoritmo individuales.

En algunas otras implementaciones, el dispositivo de comunicación de origen puede identificar una o más opciones de algoritmo de cada categoría de opción respectiva. Por ejemplo, el dispositivo de comunicación de origen puede configurarse para identificar uno o más números de grupo DH soportados o puede configurarse para soportar un algoritmo de cifrado particular (por ejemplo, Cifrado Autenticado con Datos Asociados (AEAD) con exclusión de otro algoritmo de cifrado (por ejemplo, no AEAD)).

Las opciones de algoritmo identificadas se pueden determinar con base en lo que puede soportar el dispositivo de comunicación. Por ejemplo, un dispositivo de comunicación que tenga una capacidad o habilidad computacional baja puede no ser capaz de soportar claves de 256 bits pero puede admitir claves de 128 bits. En otro ejemplo, las opciones de algoritmo identificadas pueden basarse en lo que requiere un dispositivo administrador del dispositivo de comunicación de origen. Por ejemplo, el dispositivo de comunicación de origen puede ser administrado por el dispositivo administrador y el dispositivo de administrador puede requerir que el dispositivo de comunicación de origen utilice, por ejemplo, algoritmos de Cifrado Autenticado con Datos Asociados (AEAD) al generar claves de seguridad o preparar datos. Además, las opciones de algoritmo identificados pueden basarse en lo que propone un usuario del dispositivo de comunicación de origen. Por ejemplo, un usuario puede desear que las claves que tengan un nivel de seguridad particular se usen para transformar datos para su transmisión a través de un canal de comunicación, mientras que otros usuarios de dispositivos de comunicación pueden contentarse con claves que tengan algún nivel de seguridad para poder establecer canales de comunicación seguros con un mayor número de posibles dispositivos de comunicación de destino. Por lo tanto, el dispositivo de comunicación de origen puede identificar un subconjunto de opciones de algoritmo en cada una de las categorías de opciones respectivas y, posteriormente, generar una lista de todas las combinaciones potenciales de opciones de algoritmo, donde se elige una opción de algoritmo de cada una de las categorías de opciones respectivas.

En algunas implementaciones, el dispositivo de comunicación de origen puede generar, con base en las selecciones del usuario de opciones de algoritmo, una lista de propuestas discretas para cada combinación de opciones de algoritmo. Por ejemplo, un usuario del dispositivo de comunicación de origen puede seleccionar:

Grupo HD: 15

Algoritmos de cifrado: AES-CBC-256

Algoritmos de integridad: HMAC-SHA-512-256, HMAC0SHA-384-192, HMAC-SHA-256-128, HMAC0SHA-1-96

Continuando con la implementación del ejemplo mencionado anteriormente, el dispositivo de comunicación de origen puede, posteriormente, generar cuatro propuestas discretas:

DH15 + AES-CBC-256 + HMAC-SHA-512-256

DH15 + AES-CBC-256 + HMAC-SHA-384-192

DH15 + AES-CBC-256 + HMAC-SHA-256-128

DH15 + AES-CBC-256 + HMAC-SHA-1-96

El dispositivo de comunicación de origen puede transmitir posteriormente la lista generada de propuestas discretas al dispositivo de comunicación de destino. El dispositivo de comunicación de destino puede proceder a evaluar, una por una y comenzando por el comienzo de la lista, la lista de posibles combinaciones discretas hasta el momento en que el dispositivo de comunicación de destino sea capaz de soportar una propuesta evaluada particular. En la implementación de ejemplo antes mencionada, el dispositivo de comunicación de destino puede aceptar una combinación de opciones de algoritmo tan pronto como se identifique una propuesta aceptable. Sin embargo, la aceptación por parte del dispositivo de comunicación de destino de una propuesta discreta puede ser sin tener en cuenta si la primera propuesta aceptable identificada es la combinación más segura o más eficiente de opciones de algoritmo en la lista entre las diversas combinaciones en la lista. Además, en los casos en los que el número de propuestas discretas es grande (por ejemplo, más de 4 propuestas discretas), la cantidad de transmisión de datos para transmitir las propuestas discretas puede apreciarse y ser grande.

Puede ser deseable minimizar la cantidad de tráfico de transmisión de datos entre el dispositivo de comunicación de origen y el dispositivo de comunicación de destino. También puede ser deseable que el dispositivo de comunicación de destino evalúe holísticamente opciones de algoritmo seleccionadas que tengan, por ejemplo, el mayor nivel más seguridad, en lugar de simplemente seleccionar una propuesta discreta tan pronto como sea aceptable una propuesta discreta.

La presente solicitud describe métodos para generar un número mínimo de propuestas de asociación de seguridad para que las evalúe un dispositivo de comunicación de destino mientras permite que el dispositivo de comunicación de destino identifique las opciones de algoritmo más seguras identificadas en dichas propuestas de asociación de seguridad para establecer un canal de comunicación seguro. Como será evidente en la presente descripción, cada una o más propuestas de asociación de seguridad pueden representar múltiples combinaciones de opciones de algoritmo de modo que el dispositivo de comunicación de destino pueda seleccionar y elegir opciones de algoritmo aceptables de cada una de las categorías de opciones.

En particular, las operaciones descritas en el presente documento incluyen recibir, en un dispositivo de comunicación de origen, selecciones en cada una o más categorías de opciones. Para cada categoría de opción respectiva, las operaciones incluyen la generación de una lista ordenada de opciones de algoritmo basadas en las selecciones recibidas. El dispositivo de comunicación de origen puede generar una propuesta de asociación de seguridad que incluye cada una de las respectivas categorías de opciones, donde las opciones de algoritmo en cada una de las respectivas categorías de opciones pueden estar en orden de nivel de seguridad. Una vez que la propuesta de asociación de seguridad se transmite al dispositivo de comunicación de destino, el dispositivo de comunicación de destino puede determinar la opción de algoritmo más segura de cada una de las categorías de opciones que puede soportar el dispositivo de comunicación de destino. En consecuencia, los métodos y sistemas de ejemplo que se describen a continuación pueden minimizar la cantidad de tráfico de transmisión de datos entre los dispositivos de comunicación que, de lo contrario, se requeriría para transmitir cada combinación posible de configuraciones de algoritmos de cada una de las categorías de opciones respectivas. Además, los métodos y sistemas de ejemplo que se describen a continuación pueden facilitar la evaluación holística de las opciones de algoritmos para usar al establecer un canal de comunicación seguro, mejorando así las restricciones derivadas de evaluar solo propuestas de asociación de seguridad discretas. Los ejemplos que se describen a continuación pueden aplicarse a métodos y sistemas que usan el protocolo de intercambio de claves de Internet versión 2 (IKEv2). Además, se puede apreciar que los métodos y sistemas descritos en este documento también se pueden aplicar a otras implementaciones de protocolos de seguridad de Internet.

Se hace referencia a la FIG. 1, que ilustra, en forma de diagrama de bloques, un sistema 100 para establecer un canal de comunicación seguro entre un dispositivo 110 de comunicación de origen y un dispositivo 160 de comunicación de destino, de acuerdo con un ejemplo de la presente solicitud. El sistema 100 también puede incluir un dispositivo 130 administrador. El dispositivo 130 administrador puede configurarse para gestionar el dispositivo 110 de comunicación de origen o el dispositivo 160 de comunicación de destino. En la FIG. 1, se ilustran dos dispositivos de comunicación y un dispositivo administrador; sin embargo, se puede contemplar cualquier número de dispositivos de comunicación o dispositivos administradores y se pueden configurar dos dispositivos de comunicación cualesquiera para establecer un canal de comunicación seguro para intercambiar datos. Además, en los ejemplos descritos en este documento, el dispositivo 110 de comunicación de origen puede realizar operaciones para iniciar la negociación entre los dispositivos de comunicación para establecer un canal de comunicación seguro. Sin embargo, se puede apreciar que el dispositivo 160 de comunicación de destino también puede realizar las operaciones descritas en el presente documento para establecer un canal de comunicación seguro con otros dispositivos de comunicación.

El sistema 100 incluye una red 150. El dispositivo 110 de comunicación de origen y el dispositivo 160 de comunicación de destino pueden configurarse para comunicarse entre sí a través de la red 150. Además, el dispositivo 130 administrador puede comunicarse con cualquier dispositivo de comunicación a través de la red 150 o con cualquier otro dispositivo informático similar. La red 150 puede incluir una pluralidad de redes por cable e inalámbricas interconectadas, que incluyen Internet, redes de área local, redes de área amplia o similares.

El dispositivo 110 de comunicación de origen puede establecer un canal de comunicación seguro para intercambiar datos a través de la red 150 con el dispositivo 160 de comunicación de destino. El canal de comunicación seguro puede definirse mediante opciones de algoritmo. Las opciones del algoritmo se pueden asociar con una o más categorías de opciones. Por ejemplo, las categorías de opciones pueden incluir grupos DH, algoritmos de cifrado, algoritmos de integridad o funciones pseudoaleatorias.

Las respectivas categorías de opciones pueden incluir una o más opciones de algoritmo seleccionables. Por ejemplo, los grupos DH pueden incluir los números 20, 19, 15, 14 o 0 de grupo DH. Los algoritmos de cifrado e integridad pueden incluir opciones de algoritmo seleccionables que pueden ser algoritmos AEAD o no AEAD. Las funciones pseudoaleatorias pueden incluir algoritmos HMAC-SHA. Se contemplan otras opciones de algoritmo seleccionables para establecer un canal de comunicación seguro y las opciones de algoritmos descritas en este documento se proporcionan solo como ejemplos.

El dispositivo 110 de comunicación de origen incluye uno o más procesadores, memoria y un módulo de comunicaciones para proporcionar capacidad de comunicación con otros dispositivos informáticos. La memoria puede almacenar instrucciones ejecutables por el procesador que, cuando se ejecutan, hacen que un procesador realice las operaciones descritas en este documento. En el dispositivo 110 de comunicación de origen de ejemplo descrito en este documento, la memoria puede almacenar una aplicación 112 de comunicación segura que tiene instrucciones ejecutables por procesador para realizar las operaciones descritas en este documento. Por ejemplo, la aplicación 112 de comunicación segura puede ser una aplicación de cliente de red privada virtual (VPN).

El dispositivo 110 de comunicación de origen incluye un módulo 114 de entrada/salida. En algunos ejemplos, el módulo 114 de entrada/salida puede incluir un elemento de visualización de pantalla táctil para mostrar una interfaz de usuario y una interfaz de pantalla táctil para recibir movimiento o entrada táctil de un usuario del dispositivo de comunicación. Se contemplan otros ejemplos del módulo 114 de entrada/salida para mostrar contenido para el usuario del dispositivo de comunicación y recibir señales de entrada que representan comandos u opciones seleccionables del usuario del dispositivo de comunicación.

En el ejemplo ilustrado en la FIG. 1, el dispositivo 110 de comunicación de origen puede configurarse para establecer un canal de comunicación seguro para transmitir datos y recibir datos del dispositivo 160 de comunicación de destino. Por lo tanto, el dispositivo 110 de comunicación de origen puede iniciar un proceso de negociación con el dispositivo 160 de comunicación de destino para determinar qué opciones de algoritmo usar para transmitir y recibir datos. Si las opciones de algoritmo en cualquiera de las categorías de opciones no están soportadas por el dispositivo 160 de comunicación de destino, la negociación no tendrá éxito y no se establecerá el canal de comunicación seguro. Por ejemplo, si el dispositivo 110 de comunicación de origen propone utilizar un algoritmo AEAD tanto para el cifrado como para la verificación de integridad y si el dispositivo 160 de comunicación de destino no admite algoritmos AEAD, el dispositivo 110 de comunicación de origen no podrá establecer un canal de comunicación seguro con el dispositivo 160 de comunicación de destino.

El dispositivo 130 administrador puede configurarse para gestionar dispositivos de comunicación. Por ejemplo, el dispositivo 130 administrador puede incluir una aplicación 132 administradora. La aplicación 132 administradora puede incluir instrucciones ejecutables del procesador para transmitir, al dispositivo 110 de comunicación de origen, una señal que representa un conjunto permitido de opciones de algoritmo seleccionables. El conjunto permitido de opciones de algoritmo seleccionables puede ser un subconjunto de un conjunto global de opciones de algoritmo disponibles. El conjunto permitido de opciones de algoritmo seleccionables puede ser presentado por el dispositivo 110 de comunicación de origen al usuario del primer dispositivo de comunicación. Por ejemplo, el conjunto permitido de opciones de algoritmo seleccionables puede representar el subconjunto de opciones de algoritmos que satisfacen un umbral mínimo de seguridad que el dispositivo 130 administrador exige para el dispositivo 110 de comunicación de origen . En otros ejemplos, el dispositivo 130 administrador puede determinar el conjunto permitido de opciones de algoritmo seleccionables para el dispositivo 110 de comunicación de origen con base en otros requisitos o factores.

El dispositivo 130 administrador también puede incluir registros 134 de datos. Los registros 134 de datos pueden almacenarse en la memoria del dispositivo 130 administrador. Los registros 134 de datos pueden incluir datos asociados con los dispositivos de comunicación respectivos que son administrados por el dispositivo administrador 130. Por ejemplo, el dispositivo 130 administrador puede incluir un registro de datos asociado con el dispositivo 110 de comunicación de origen . En un ejemplo, el registro de datos puede identificar al usuario del dispositivo 110 de comunicación de origen como un arquitecto técnico de una empresa de tecnología. El usuario del primer dispositivo 110 de comunicación puede transmitir rutinariamente, a través de correo electrónico, secretos comerciales de la empresa. En consecuencia, el registro de datos asociado con el dispositivo 110 de comunicación de origen puede incluir instrucciones que requieran que el conjunto permitido de algoritmos seleccionables para el dispositivo 110 de comunicación de origen incluya algoritmos de cifrado e integridad que tengan una longitud de clave igual o superior a 256 bits. En algunos ejemplos, el dispositivo 130 administrador puede transmitir una señal al primer dispositivo 110 de comunicación que indica que al menos algunas opciones de algoritmo en una interfaz de usuario, como se describe en el presente documento, deben preseleccionarse como opciones de algoritmo seleccionadas. En algunos ejemplos, la señal al primer dispositivo 110 de comunicación puede indicar que al menos algunas de las opciones de algoritmo preseleccionadas pueden no ser deseleccionadas. Es decir, en el escenario anterior del usuario arquitecto técnico, al menos algunas opciones del algoritmo pueden no ser deseleccionadas (por ejemplo, son obligatorias). Se contemplan

otros criterios para identificar el conjunto permitido de opciones de algoritmo seleccionables para un dispositivo de comunicación particular.

Se puede apreciar que el dispositivo 160 de comunicación de destino puede ser similar al dispositivo 110 de comunicación de origen y que el dispositivo 160 de comunicación de destino puede realizar las operaciones de ejemplo descritas en el presente documento para establecer un canal de comunicación seguro con el dispositivo 110 de comunicación de origen.

Se hace referencia a la FIG. 2, que ilustra, en forma de diagrama de flujo, un método 200 para establecer un canal de comunicación seguro entre el dispositivo 110 de comunicación de origen (FIG. 1) y el dispositivo 160 de comunicación de destino (FIG. 1), de acuerdo con un ejemplo de la presente solicitud. El método 200 incluye operaciones que pueden ser realizadas por uno o más procesadores del dispositivo 110 de comunicación de origen. Por ejemplo, el método 200 puede implementarse, al menos en parte, a través de instrucciones ejecutables por procesador asociadas con la aplicación 112 de comunicación segura (FIG. 1). En algunos ejemplos, una o más de las operaciones pueden implementarse a través de instrucciones ejecutables por procesador en otras aplicaciones o en un sistema operativo almacenado y ejecutado en el dispositivo 110 de comunicación de origen. Como se describirá, el dispositivo 110 de comunicación de origen incluye un módulo 114 entrada / salida (FIG. 1) que puede incluir un elemento de visualización para mostrar una interfaz de usuario y un módulo de entrada para recibir selecciones.

En la operación 210, el dispositivo 110 de comunicación de origen muestra, en un elemento de visualización, una interfaz de usuario que incluye opciones de algoritmo seleccionables. En algunos ejemplos, la interfaz de usuario puede incluir una lista de las posibles opciones de algoritmo disponibles para establecer un canal de comunicación seguro. En algunos ejemplos, la lista de posibles opciones de algoritmos se puede agrupar según la categoría de opción. Es decir, las opciones de grupo DH se pueden agrupar en un área de la interfaz de usuario, las opciones de algoritmo de cifrado se pueden agrupar en otra área de la interfaz de usuario, las opciones de algoritmo de integridad se pueden agrupar en un área adicional de la interfaz de usuario y las opciones de función pseudoaleatoria se pueden agrupar en alguna otra área de la interfaz de usuario. El dispositivo 110 de comunicación de origen puede proporcionar elementos de interfaz de usuario, como casillas de verificación, botones pulsadores o similares, para que un usuario seleccione las opciones de algoritmo deseadas. Se pueden contemplar otras implementaciones de interfaz de usuario.

En la operación 220, el dispositivo 110 de comunicación de origen recibe, a través de un módulo de entrada, una señal que representa una o más selecciones de opciones de algoritmo. Por ejemplo, si el módulo 114 de entrada/salida es un elemento de visualización táctil y la interfaz de usuario incluye una o más casillas de verificación junto a las opciones de algoritmo disponibles, el dispositivo 110 de comunicación de origen puede recibir entradas de pantalla táctil de selecciones de opciones de algoritmo cuando un usuario selecciona casillas de verificación asociadas con las opciones deseadas del algoritmo.

En algunos ejemplos, la respectiva una o más selecciones pueden asociarse con una de una o más categorías de opciones. Por ejemplo, una opción de algoritmo AES-GCM-128 se puede asociar tanto con una categoría de algoritmo de cifrado como con una categoría de algoritmo de integridad. En otro ejemplo, una opción de algoritmo HMAC-SHA-512-256 mostrada se puede asociar con una categoría de algoritmo de integridad. La Tabla 1 (a continuación) ilustra categorías de opciones de ejemplo y opciones de algoritmos de ejemplo asociadas con una o más categorías de opciones.

Tabla 1: Categorías de Opciones de Ejemplo y Opciones de Algoritmo

Categoría de Opción	Opción de Algoritmo
Grupos DH	20
	19
	15
	14
	ninguno
Algoritmos de cifrado	AES-GCM-256
	AES-GCM-128

Categoría de Opción	Opción de Algoritmo
	AES-CBC-256
	AES-CBC-128
	Poly1305-Chacha20
	Sin encriptación
Algoritmos de integridad	AES-GCM-256
	AES-GCM-128
	HMAC-SHA-512-256
	HMAC-SHA-384-192
	HMAC-SHA-256-128
	HMAC-SHA-1-96
Funciones pseudoaleatorias	HMAC-SHA-512
	HMAC-SHA-384
	HMAC-SHA-256
	HMAC-SHA-1

En algunos ejemplos, el dispositivo 110 de comunicación de origen puede proporcionar una interfaz de usuario con selecciones de opciones de algoritmo predeterminadas. Por ejemplo, el dispositivo 110 de comunicación de origen puede proporcionar a la interfaz de usuario las opciones de algoritmo AES-GCM seleccionadas (por ejemplo, casillas de verificación asociadas con la matriz de algoritmos AES-GCM seleccionada). En algunos ejemplos, las selecciones predeterminadas de opciones de algoritmo pueden estar asociadas con un nivel de seguridad mínima en el que el dispositivo 110 de comunicación de origen está obligado a operar.

En algunos ejemplos, las selecciones de opciones de algoritmo predeterminadas descritas anteriormente pueden basarse en opciones soportadas por el dispositivo 110 de comunicación de origen. Por ejemplo, el dispositivo 110 de comunicación de origen puede determinar si el dispositivo 110 de comunicación de origen puede calcular claves de 256 bits de longitud. Por lo tanto, en la operación 210, la interfaz de usuario visualizada puede incluir un conjunto soportado de opciones de algoritmo seleccionables y puede no incluir opciones de algoritmos que no estén dentro de dicho conjunto admitido. En un ejemplo alternativo, las opciones de algoritmo que no están dentro de dicho conjunto soportado pueden mostrarse pero no pueden ser seleccionables. En algunos ejemplos, la una o más selecciones recibidas (por ejemplo, la operación 220) pueden ser un subconjunto del conjunto soportado de opciones de algoritmo seleccionables.

En algunos ejemplos, las selecciones de opciones de algoritmos predeterminadas descritas anteriormente pueden basarse en opciones ordenadas por el dispositivo 130 administrador. En algunos ejemplos, las opciones de algoritmo predeterminadas no pueden ser deseleccionables. Es decir, es posible que el usuario del dispositivo 110 de comunicación de origen no pueda anular la selección de una o más opciones de algoritmo con base en las reglas proporcionadas por el dispositivo 130 administrador. Por ejemplo, el dispositivo 130 administrador puede requerir que las operaciones para establecer y comunicarse a través del canal de comunicación seguro utilizan la función pseudoaleatoria HMAC-SHA-512. Además, el usuario del dispositivo 110 de comunicación de origen puede realizar al menos una selección de una o más opciones de algoritmo no predeterminadas. Es decir, para las opciones de algoritmo que no son opciones de algoritmo predeterminadas, el dispositivo 110 de comunicación de origen puede recibir, a través de un módulo de entrada, una señal que representa una o más selecciones de una lista de opciones de algoritmo no predeterminadas.

En algunos ejemplos, el dispositivo 110 de comunicación de origen puede recibir, desde el dispositivo 130 administrador, una señal que representa un conjunto permitido de opciones de algoritmo seleccionables. El conjunto permitido de opciones de algoritmo seleccionables puede ser un subconjunto de un conjunto global de opciones de algoritmo disponibles. Por lo tanto, en respuesta a la recepción de la señal que representa un conjunto permitido de opciones de algoritmo seleccionables, el dispositivo 110 de comunicación de origen puede mostrar una interfaz de usuario que incluye opciones de algoritmo que se adhieren a un estándar de seguridad mínimo definido por el dispositivo 130 administrador. En algunos ejemplos, las selecciones recibidas o más (por ejemplo, la operación 220) pueden ser un subconjunto del conjunto permitido de opciones de algoritmo seleccionables.

En la operación 230, para las respectivas categorías de opciones, el dispositivo 110 de comunicación de origen puede generar una lista ordenada de opciones de algoritmos con base en las selecciones recibidas. En algunos ejemplos, el dispositivo 110 de comunicación de origen puede ordenar las opciones de algoritmo en orden de nivel de seguridad.

Para ilustrar, el dispositivo 110 de comunicación de origen puede haber recibido una señal que represente la selección de opciones de algoritmo descritas en la Tabla 2 (a continuación). El dispositivo 110 de comunicación de origen puede generar una lista clasificada en orden de nivel de seguridad decreciente (o creciente). En algunos ejemplos, el orden del nivel de seguridad puede determinarse con base en el número de bits de clave de seguridad o del número de bits de información asociados con los algoritmos de cifrado/integridad. En algunos otros ejemplos, el orden del nivel de seguridad puede determinarse con base en reglas almacenadas en el dispositivo 110 de comunicación de origen . Por ejemplo, los números de grupo DH pueden ordenarse en orden descendente u otro orden basado en reglas. Aunque la Tabla 2 ilustra algunos ejemplos en los que las opciones de algoritmo seleccionadas se clasifican en orden decreciente de seguridad, se pueden contemplar otros criterios para generar la lista ordenada de opciones de algoritmo.

Tabla 2: Ejemplo de Selección Recibida de Opciones de Algoritmo

	Selección Recibida de Opciones de Algoritmo	Lista Ordenada de Opciones de Seguridad
Grupos DH	14	20
	20	15
	15	14
Algoritmos de cifrado	AES-CBC-128	AES-GCM-256 / AES-CBC-256
	AES-CBC-256	AES-GCM-128 / AES-CBC-128
	AES-GCM-128	
	AES-GCM-256	
Algoritmos de integridad	HMAC-SHA-1-96	HMAC-SHA-512-256
	HMAC-SHA-256-128	HMAC-SHA-384-192
	HMAC-SHA-384-192	HMAC-SHA-256-128
	HMAC-SHA-512-256	HMAC-SHA-1-96
	AES-GCM-128	
	AES-GCM-256	
Funciones pseudoaleatorias	HMAC-SHA-1	HMAC-SHA-512
	HMAC-SHA-256	HMAC-SHA-384

	Selección Recibida de Opciones de Algoritmo	Lista Ordenada de Opciones de Seguridad
	HMAC-SHA-384	HMAC-SHA-256
	HMAC-SHA-512	HMAC-SHA-1

Como se ilustra en el ejemplo de la Tabla 2, el dispositivo 110 de comunicación de origen puede clasificar los números del grupo DH según un orden numérico descendente; sin embargo, se puede apreciar que se contemplan otros métodos de clasificación de los números DH. El dispositivo 110 de comunicación de origen puede clasificar los algoritmos de cifrado seleccionados del más seguro al menos seguro (por ejemplo, un algoritmo de cifrado que usa claves que tienen una longitud de clave de 256 puede ser más seguro que un algoritmo de cifrado que usa claves que tienen una longitud de clave de 128). El dispositivo 110 de comunicación de origen puede ordenar los algoritmos de integridad seleccionados del más seguro al menos seguro. Además, el dispositivo 110 de comunicación de origen puede clasificar las funciones pseudoaleatorias seleccionadas desde la más segura hasta la menos segura.

En la operación 240, el dispositivo 110 de comunicación de origen puede generar una o más propuestas de asociación de seguridad que incluyen una o más de las opciones de algoritmo de cada una de las respectivas listas ordenadas de opciones de algoritmo. Es decir, una propuesta de asociación de valores de ejemplo puede incluir al menos una opción de algoritmo elegida de cada una de las categorías de opciones. Las propuestas de asociación de seguridad se generan con base en un orden en la lista ordenada de algoritmos. Por ejemplo, la lista ordenada de algoritmos puede estar en orden de nivel de seguridad.

Continuando con el ejemplo descrito anteriormente de la Tabla 2, el dispositivo 110 de comunicación de origen puede generar dos propuestas, ilustradas en la Tabla 3 (a continuación).

Tabla 3: Propuestas de Asociaciones de Seguridad de Ejemplo

Propuesta 1	**Propuesta 2**
grupo 20 DH	grupo 20 DH
grupo 19 DH	grupo 19 DH
grupo 15 DH	grupo 15 DH
grupo 14 DH	grupo 14 DH
Cifrado AES-GCM, longitud de clave 256	Cifrado AES-CBC, longitud de clave 256
Cifrado AES-GCM, longitud de clave 128	Cifrado AES-CBC, longitud de clave 128
Función pseudoaleatoria HMAC-SHA-512	Integridad HMAC-SHA-512-256
Función pseudoaleatoria HMAC-SHA-384	Integridad HMAC-SHA-384-192
Función pseudoaleatoria HMAC-SHA-256	Integridad HMAC-SHA-256-128
Función pseudoaleatoria HMAC-SHA-1	Integridad HMAC-SHA-1-96
	Función pseudoaleatoria HMAC-SHA-512
	Función pseudoaleatoria HMAC-SHA-384
	Función pseudoaleatoria HMAC-SHA-256
	Función pseudoaleatoria HMAC-SHA-1

En el ejemplo de la Tabla 3, el dispositivo 110 de comunicación de origen genera un número mínimo de propuestas de asociación de seguridad que incluyen una combinación de opciones de algoritmo que son compatibles y que son representativas de al menos una opción de algoritmo de cada una de las categorías de opciones. La una o más propuestas de asociación de seguridad se generan con base en un orden en la lista ordenada. Por ejemplo, como se ilustra en la Tabla 3, cada una de las categorías de opciones respectivas se clasifican en orden decreciente de nivel de seguridad. Se puede apreciar que debido a que las respectivas propuestas de asociación de seguridad incluyen el orden en la lista ordenada asociada, el dispositivo 160 de comunicación de destino puede identificar las características de la opción de algoritmo (por ejemplo, el nivel de seguridad) sin tener que recorrer la lista completa de opciones de algoritmo para identificar, por ejemplo. ejemplo, la opción de fuerza de seguridad más segura.

En el ejemplo de la Tabla 3, se proporcionan dos propuestas, donde cada propuesta incluye opciones de algoritmo que pueden ser compatibles entre sí. Además, en el ejemplo descrito anteriormente asociado con la Tabla 3, se proporcionan un mínimo de dos propuestas al menos porque las opciones de algoritmo AEAD no se pueden combinar en una propuesta de asociación de seguridad con opciones de algoritmo no AEAD. El dispositivo 110 de comunicación de origen genera una primera propuesta que incluye una lista ordenada de selecciones de algoritmos de cifrado AEAD (por ejemplo, cifrado AES-GCM con longitudes de clave 256 y 128). Puede apreciarse que cuando se realiza una selección de algoritmo de cifrado AEAD, puede no ser necesaria una selección de algoritmo de integridad.

Además, debido a que los algoritmos de integridad que no son AEAD (por ejemplo, las opciones de algoritmos de la familia HMAC-SHA) pueden ser incompatibles con los algoritmos AEAD, los algoritmos de integridad que no son AEAD se incluyen en una segunda propuesta. En el ejemplo ilustrado en la Tabla 3, la primera propuesta incluye selecciones de opciones de algoritmos AEAD (por ejemplo, opciones de algoritmos de la familia AES-GCM) con exclusión de los algoritmos de integridad que no son AEAD. Además, la segunda propuesta incluye los algoritmos de integridad no AEAD con exclusión de los algoritmos AEAD. En consecuencia, el dispositivo 110 de comunicación de origen puede determinar si las selecciones de opciones de algoritmos en una categoría de opciones son compatibles/operables con selecciones de opciones de algoritmos en otra categoría de opciones. Por tanto, el dispositivo 110 de comunicación de origen puede generar un número mínimo de propuestas necesarias para incluir cada opción de algoritmo seleccionada en al menos una propuesta de asociación de seguridad. En los ejemplos anteriores, el dispositivo 110 de comunicación de origen genera un número mínimo de propuestas y no genera una pluralidad de propuestas discretas para representar todas las permutaciones/combinaciones de opciones de algoritmo. En consecuencia, el dispositivo 110 de comunicación de origen proporciona propuestas compactas al negociar el establecimiento de un canal de comunicación seguro con el dispositivo 160 de comunicación de destino.

Se puede apreciar que si, en la operación 220, el dispositivo 110 de comunicación de origen recibe una señal que representa selecciones que solo incluyen opciones de algoritmo AEAD, entonces el dispositivo 110 de comunicación de origen puede generar una sola propuesta de asociación de seguridad para incluir opciones de algoritmo de cada una de las categorías de opciones.

En la operación 250, el dispositivo 110 de comunicación de origen puede transmitir una o más propuestas de asociación de seguridad al dispositivo 160 de comunicación de destino para establecer el canal de comunicación seguro a través de la red 150.

Además, el dispositivo 110 de comunicación de origen puede recibir una señal del dispositivo 160 de comunicación de destino que indica que se ha seleccionado una o más propuestas de asociación de seguridad. En respuesta a la recepción de esta señal del dispositivo 160 de comunicación de destino, el dispositivo 110 de comunicación de origen puede establecer la comunicación segura con el dispositivo 160 de comunicación de destino para transmitir datos y recibir datos desde ese dispositivo 160 de comunicación de destino.

Por ejemplo, el dispositivo 110 de comunicación de origen puede recibir una señal del dispositivo 160 de comunicación de destino que indica que cada una de las opciones de algoritmo de nivel de seguridad más alto de cada una de las categorías de opciones respectivas o que cada una de las opciones de algoritmo clasificadas más altas en la lista ordenada de opciones de seguridad está soportada por el dispositivo de comunicación de destino (por ejemplo, una opción de algoritmo de cada categoría de opciones). El dispositivo 110 de comunicación de origen puede preparar datos para la transmisión con base en las opciones de algoritmo de nivel de seguridad más alto que están soportadas por el dispositivo 160 de comunicación de destino y, posteriormente, transmitir los datos preparados al dispositivo 160 de comunicación de destino a través del canal de comunicación seguro establecido. Por ejemplo, la preparación de datos para la transmisión puede incluir la identificación de claves asociadas con un número de grupo DH y el cifrado de datos usando el algoritmo de cifrado identificado en la propuesta de asociación de seguridad. Además, preparar los datos para la transmisión también puede incluir agregar firmas digitales o similares según el algoritmo de integridad identificado en la propuesta de asociación de seguridad o utilizar la función pseudoaleatoria identificada para las operaciones descritas en este documento.

En algunos ejemplos, el dispositivo 110 de comunicación de origen puede actualizar dinámicamente la interfaz de usuario para mostrar opciones de algoritmo seleccionables. Por ejemplo, una vez que se muestra una interfaz de usuario en el dispositivo 110 de comunicación de origen (por ejemplo, la operación 210, FIG. 2), el dispositivo 110 de comunicación de origen puede determinar que se selecciona un algoritmo AEAD (por ejemplo, algoritmo de cifrado AES-GCM) de la interfaz de usuario (por ejemplo, la operación 220, FIG. 2) y, en respuesta, puede restringir la

generación de propuestas de asociación de seguridad para que no incluya algoritmos de integridad no AEAD (por ejemplo, algoritmos de la familia HMAC-SHA). Es decir, es posible que los algoritmos de integridad no AEAD ya no estén disponibles para su selección a través de la interfaz de usuario que se muestra.

En otro ejemplo, una vez que se muestra una interfaz de usuario que incluye opciones de algoritmo seleccionables en el dispositivo 110 de comunicación de origen, el dispositivo 110 de comunicación de origen puede determinar que una o más selecciones de opciones de algoritmo es un algoritmo de integridad no AEAD y, en respuesta, puede seleccionar automáticamente uno o más algoritmos de cifrado no AEAD de un conjunto global de opciones de algoritmo disponibles. En algunos ejemplos, los algoritmos de cifrado que no son AEAD incluyen la familia AES-CBC de algoritmos de cifrado.

Ahora se hace referencia a la FIG. 3, que ilustra esquemáticamente una interfaz 300 de usuario que incluye opciones de algoritmo seleccionables, de acuerdo con un ejemplo de la presente solicitud. La interfaz 300 de usuario puede ser proporcionada por la aplicación 112 de comunicación segura (FIG. 1) que se ejecuta en el dispositivo 110 de comunicación de origen (FIG. 1). En el presente ejemplo, la interfaz 300 de usuario es para recibir la selección de usuario de uno o más algoritmos 310 de cifrado y uno o más algoritmos 320 de integridad. Las selecciones de usuario pueden realizarse mediante la entrada de casillas de verificación. En otros ejemplos se contemplan otros mecanismos de entrada, como iconos, etc. Por ejemplo, el dispositivo 110 de comunicación de origen puede, en la operación 210, mostrar la interfaz 300 de usuario que incluye los algoritmos 310 de cifrado seleccionables y uno o más algoritmos 320 de integridad seleccionables. Posteriormente, el dispositivo 110 de comunicación de origen puede, en la operación 220, recibir información del usuario. entrada a través de las casillas de verificación para indicar la selección de algoritmos de cifrado requeridos o algoritmos de integridad. Puede apreciarse que la interfaz 300 de usuario ilustra algoritmos 310 de cifrado y algoritmos 320 de integridad; sin embargo, también se pueden mostrar otras opciones de algoritmo.

Para ilustrar algunos de los ejemplos anteriores, en la interfaz 300 de usuario de la FIG. 3, el usuario del dispositivo 110 de comunicación de origen puede seleccionar la opción de algoritmo AES-GCM-256 en la categoría "Algoritmos de Cifrado". En respuesta, el dispositivo 110 de comunicación de origen puede seleccionar automáticamente la opción de algoritmo AES-GCM-256 en "Algoritmos de Integridad". Se puede apreciar que la selección visual de la opción de algoritmo en la categoría "Algoritmos de Integridad" es ilustrativa para el usuario del dispositivo, ya que el protocolo AES-GCM-256 no necesariamente requiere que se seleccione una opción de algoritmo de integridad una vez que la opción del algoritmo de cifrado correspondiente es seleccionada.

Además, en la interfaz 300 de usuario de la FIG. 3, el usuario del dispositivo 110 de comunicación de origen puede seleccionar opciones de algoritmo AEAD (por ejemplo, AES-GCM-256) y opciones de algoritmo no AEAD (por ejemplo, AES-CBC-256 o AES-CBC-128). En los ejemplos descritos en este documento, cuando se seleccionan tanto las opciones de algoritmo AEAD como las opciones de algoritmo no AEAD, el dispositivo 110 de comunicación de origen puede generar dos o más propuestas de asociación de seguridad, ya que puede ser inoperable para incluir una opción de algoritmo de cifrado AEAD con un algoritmo no AEAD. opción de algoritmo de integridad dentro de la misma propuesta de asociación de seguridad. En consecuencia, en el presente ejemplo, el dispositivo 110 de comunicación de origen puede generar dos o más propuestas de asociación de seguridad.

Ahora se hace referencia a la FIG. 4, que ilustra esquemáticamente una interfaz 400 de usuario, de acuerdo con un ejemplo de la presente solicitud. El dispositivo 110 de comunicación de origen (FIG. 1) puede generar la interfaz 400 de usuario después de recibir una señal que representa una o más selecciones a través del módulo de entrada. Por ejemplo, el dispositivo 110 de comunicación de origen puede generar la interfaz 400 de usuario en la FIG. 4 al recibir una señal que representa una o más selecciones de opciones de algoritmo. El dispositivo 110 de comunicación de origen puede generar la interfaz 400 de usuario de la FIG. 4 para resumir las selecciones 430 de opciones de algoritmo que corresponden a las selecciones recibidas de un usuario que proporcionó una entrada usando la interfaz 300 de usuario en la FIG. 3.

Además, en algunos ejemplos, la interfaz 400 de usuario puede incluir una interfaz 440 de entrada de alternancia para recibir instrucciones para generar una propuesta de asociación de seguridad (por ejemplo, la operación 240 de la FIG. 2). Por ejemplo, cuando la interfaz 440 de entrada de alternancia se establece en una posición "activada", el dispositivo 110 de comunicación de origen puede generar una o más propuestas de asociación de seguridad como si todas las opciones de algoritmo estuvieran seleccionadas. Es decir, cuando la interfaz 440 de entrada de alternancia se establece en una posición "activada", el dispositivo 110 de comunicación de origen puede generar una o más propuestas de asociación de seguridad como si cada algoritmo 310 de cifrado (FIG. 3) estuviera seleccionado y como si cada integridad se selecciona el algoritmo 320 (FIG. 3). Un usuario del dispositivo de comunicación de origen puede configurar la interfaz 440 de entrada de alternancia en la posición "activada" cuando el usuario no está interesado en utilizar algoritmos específicos para establecer un canal de comunicación seguro con un dispositivo 160 de comunicación de destino (FIG. 1). En algunos ejemplos, la posición "encendido" puede conocerse como un modo "compatible", ya que el modo "compatible" puede aumentar las posibilidades de que una o más propuestas de asociación de seguridad transmitidas al dispositivo 160 de comunicación de destino estén soportadas o aceptadas por el dispositivo 160 de comunicación de destino.

Cuando la interfaz 440 de entrada de alternancia se establece en una posición de "apagado", el dispositivo 110 de comunicación de origen puede generar una propuesta de asociación de seguridad de acuerdo con uno o más métodos descritos en el presente documento. Es decir, cuando la interfaz 440 de entrada de alternancia se establece en una posición de "apagado". ', el dispositivo 110 de comunicación de origen identifica qué opciones de algoritmo específico incorporar en una propuesta de asociación de seguridad basada en las opciones de selección del usuario, como las selecciones de opción 430 de algoritmo que se muestran en la FIG. 4.

En los ejemplos descritos en este documento, el dispositivo 110 de comunicación de origen puede generar una propuesta de asociación de seguridad que tiene una pluralidad de listas ordenadas de opciones de algoritmo (por ejemplo, ordenadas en orden de medición de la fuerza de la seguridad), donde cada lista ordenada está asociada con una categoría de opción (por ejemplo, número de grupo DH, algoritmo de cifrado, etc.). El dispositivo 110 de comunicación de origen puede transmitir la propuesta de asociación de seguridad generada al dispositivo 160 de comunicación de destino. Posteriormente, el dispositivo 160 de comunicación de destino puede identificar o elegir una opción de algoritmo que el dispositivo 160 de comunicación de destino puede soportar de cada una de las categorías de opciones. Por lo tanto, se puede establecer un canal de comunicación seguro entre el dispositivo 110 de comunicación de origen y el dispositivo 160 de comunicación de destino. Es decir, el dispositivo 160 de comunicación de destino puede identificar opciones de algoritmo a partir de una sola ronda de generación de propuestas. Además, el dispositivo 160 de comunicación de destino puede identificar eficientemente, con base en una lista ordenada de opciones de algoritmo para cada una de las categorías de opciones, las opciones de algoritmo que tienen el mayor nivel de seguridad soportada o con base en otros criterios basados en reglas. Es decir, si la opción de nivel de seguridad más alto no está soportada por el dispositivo 160 de comunicación de destino, el dispositivo 160 de comunicación de destino puede seleccionar la siguiente opción de nivel de seguridad inferior en la lista ordenada de opciones de algoritmo para esa categoría de opciones. Se puede apreciar que si el dispositivo 160 de comunicación de destino no puede soportar ninguna de las selecciones de opciones de algoritmo del dispositivo 110 de comunicación de origen , el dispositivo 160 de comunicación de destino puede identificar, poco después de que se proporcione la propuesta o propuestas de asociación de seguridad, que no se puede establecer un canal de comunicación seguro entre los respectivos dispositivos de comunicación.

Se hace referencia a la FIG. 5, que ilustra, en forma de diagrama de bloques simplificado, un dispositivo 500 electrónico, de acuerdo con un ejemplo de la presente solicitud. El dispositivo 500 electrónico puede ser el dispositivo 110 de comunicación de origen (FIG. 1), el dispositivo 160 de comunicación de destino (FIG. 1), o el dispositivo 130 administrador (FIG. 1).

El dispositivo 500 electrónico incluye uno o más procesadores 502, memoria 504 y un módulo de comunicaciones para proporcionar capacidades de comunicación en red con otros dispositivos informáticos. La memoria 504 puede almacenar aplicaciones de software ejecutables por el procesador 506 que incluyen un sistema operativo para proporcionar funciones básicas del dispositivo. Las aplicaciones 506 de software también pueden contener instrucciones que implementan las operaciones y funciones de los métodos descritos en este documento. Por ejemplo, en el caso del dispositivo 110 de comunicación de origen , las aplicaciones 506 de software pueden incluir la aplicación 112 de comunicación segura (FIG. 1) u operaciones de ejemplo ilustradas con referencia al método 200 de la FIG. 2.

El dispositivo 500 electrónico incluye una interfaz de elemento de visualización y/o un elemento de visualización 508. El elemento de visualización 508 puede ser cualquier elemento de visualización adecuado, como un elemento de visualización de cristal líquido (LCD), un elemento de visualización de tinta electrónica/papel electrónico o similar. En algunos ejemplos, el elemento de visualización 508 es un elemento de visualización táctil.

El dispositivo 500 electrónico incluye un módulo 510 de entrada para recibir señales que representan comandos o selecciones consistentes con los ejemplos descritos en el presente documento. Por ejemplo, el dispositivo 500 electrónico puede recibir, a través del módulo 510 de entrada, una señal que representa una o más selecciones, donde la respectiva una o más selecciones están asociadas con una de una o más categorías de opciones, como se describe en el presente documento. En algunos ejemplos, el módulo 510 de entrada puede ser un módulo de interfaz de entrada táctil de una pantalla táctil, una entrada de botón pulsador, una entrada de dispositivo señalador u otro dispositivo similar. En algunos ejemplos, la combinación del elemento de visualización 508 y el módulo 510 de entrada corresponde al módulo 114 de entrada/salida de la FIG. 1.

En algunos ejemplos, el dispositivo 500 electrónico es un dispositivo electrónico portátil, como un teléfono inteligente, un ordenador personal, un asistente digital personal, un dispositivo de navegación portátil, un teléfono móvil, un dispositivo informático portátil (por ejemplo, reloj inteligente, monitor de actividad portátil , o similares), o cualquier otro tipo de dispositivo informático que pueda configurarse para almacenar datos e instrucciones de software, y ejecutar instrucciones de software para realizar operaciones de ejemplo descritas en el presente documento.

Las realizaciones de ejemplo de la presente solicitud no se limitan a ningún sistema operativo, arquitectura de sistema, arquitectura de dispositivo móvil, arquitectura de servidor o lenguaje de programación informático en particular.

Se entenderá que las aplicaciones, módulos, rutinas, procesos, subprocesos u otros componentes de software que implementen el método/proceso descrito pueden realizarse usando técnicas y lenguajes de programación informática estándar. La presente solicitud no se limita a procesadores particulares, lenguajes informáticos, convenciones de programación informática, estructuras de datos u otros detalles de implementación similares. Los expertos en la técnica reconocerán que los procesos descritos pueden implementarse como parte de un código ejecutable por ordenador almacenado en una memoria volátil o no volátil, como parte de un chip integrado de aplicación específica (ASIC), etc.

Se pueden realizar ciertas adaptaciones y modificaciones de las realizaciones descritas. Por lo tanto, las realizaciones discutidas anteriormente se consideran como ilustrativas y no restrictivas.

REIVINDICACIONES

1. Un método (200) para establecer un canal de comunicación seguro entre un primer dispositivo (110) de comunicación y un segundo dispositivo (160) de comunicación, estando definido el canal de comunicación seguro por una o más opciones de algoritmo, estando la una o más opciones de algoritmo asociadas con una de una o más categorías de opciones, estando realizado el método en el primer dispositivo (110) de comunicación que comprende:

recibir (220), a través de un módulo de entrada, una señal que representa una o más selecciones, estando la respectiva una o más selecciones asociadas con una de las una o más categorías de opciones;

para las respectivas categorías de opciones, generar (230) una lista ordenada de opciones de algoritmos en orden de nivel de seguridad con base en las selecciones recibidas;

generar (240) una propuesta de asociación de seguridad que incluye una o más de las opciones de algoritmo de las respectivas listas ordenadas de opciones de algoritmo, en donde la propuesta de asociación de seguridad se genera con base en un orden en la lista ordenada de opciones de algoritmo; y

transmitir (250) la propuesta de asociación de seguridad al segundo dispositivo de comunicación para establecer el canal de comunicación seguro.

2. El método de la reivindicación 1, que comprende además mostrar (210), en un elemento de visualización, una interfaz (300, 400) de usuario que incluye opciones (310, 320) de algoritmo seleccionables, y en donde la interfaz de usuario incluye una opción de algoritmo seleccionada predeterminada.

3. El método de la reivindicación 2, en donde la opción de algoritmo seleccionada predeterminada no es deseleccionable, y en donde una o más selecciones incluyen una opción de algoritmo no predeterminada.

4. El método de la reivindicación 1, que comprende además: recibir, desde un dispositivo (130) administrador, una señal que representa un conjunto permitido de opciones de algoritmo seleccionables, y en donde el conjunto permitido de opciones de algoritmo seleccionables es un subconjunto de un conjunto global de opciones de algoritmo disponibles, y en donde una o más selecciones son un subconjunto del conjunto permitido de opciones de algoritmo seleccionables en la interfaz de usuario.

5. El método de la reivindicación 1, que comprende además:

determinar un conjunto soportado de opciones de algoritmo que están soportadas por el primer dispositivo (110) de comunicación,

y en donde una o más selecciones son un subconjunto del conjunto soportado de opciones de algoritmo seleccionables en la interfaz de usuario.

6. El método de la reivindicación 1, que comprende además:

recibir una señal, desde el segundo dispositivo (160) de comunicación, que indica que las opciones de algoritmo asociadas con la propuesta de asociación de seguridad están soportadas por el segundo dispositivo de comunicación; y

preparar los datos con base en las opciones de algoritmo de la propuesta de asociación de seguridad y, posteriormente, transmitir los datos preparados al segundo dispositivo de comunicación por el canal de comunicación seguro.

7. El método de la reivindicación 1, en donde una o más categorías de opciones incluyen una categoría de algoritmo de cifrado y una categoría de algoritmo de integridad, y en donde la categoría de algoritmo de cifrado incluye un algoritmo de Cifrado Autenticado con Datos Asociados, AEAD, y en donde generar la propuesta de asociación de seguridad incluye:

determinar que se seleccione un algoritmo AEAD desde la interfaz de usuario y, en respuesta, restringir la generación de propuestas de asociación de seguridad para que no incluya algoritmos de integridad no AEAD.

8. El método de la reivindicación 7, en donde el algoritmo AEAD incluye algoritmos Galois Estándar de Cifrado Avanzado /Modo Contador, AES-GCM.

9. El método de la reivindicación 1, en donde una o más categorías de opciones incluyen una categoría de algoritmo de cifrado y una categoría de algoritmo de integridad, y en donde la generación de la propuesta de asociación de seguridad incluye:

determinar que una o más selecciones de opciones de algoritmo de integridad son algoritmos de integridad de cifrado no autenticado con datos asociados, no AEAD y, en respuesta, seleccionar automáticamente uno o más algoritmos de cifrado no AEAD de un conjunto global de opciones de algoritmo disponibles.

10. El método de la reivindicación 9, en donde un algoritmo de integridad no AEAD incluye el Algoritmo Hash Seguro de Código de Autenticación de Mensajes basado en Hash, HMAC-SHA, y en donde un algoritmo de cifrado no AEAD incluye el Algoritmo de Cifrado Estándar de Encriptado Avanzado en el Modo de Encadenamiento de Bloques de Cifrado, AES-CBC.

11. El método de la reivindicación 1, en donde una o más categorías de opciones incluyen al menos uno de un grupo Diffie-Hellman, algoritmo de cifrado, algoritmo de integridad o función pseudoaleatoria.

12. Un dispositivo (500) informático que comprende:

un módulo de comunicaciones;

un módulo (510) de entrada;

un elemento de visualización (508);

un procesador (502) acoplado al módulo de comunicaciones, el elemento de visualización y el módulo de entrada; y

una memoria (504) acoplada al procesador, almacenando la memoria instrucciones ejecutables por el procesador para establecer un canal de comunicación seguro entre el dispositivo informático y un segundo dispositivo (160) de comunicación, estando definido el canal de comunicación seguro por una o más opciones de algoritmo, estando asociadas la una o más opciones de algoritmo con una de una o más categorías de opciones, en las que las instrucciones ejecutables por el procesador, cuando se ejecutan, configuran el procesador para llevar a cabo el método de cualquiera de las reivindicaciones anteriores.

13. Un programa informático que, cuando es ejecutado por un procesador (502) de un sistema (500) informático, hace que el sistema informático lleve a cabo el método de una cualquiera de las reivindicaciones 1 a 11.

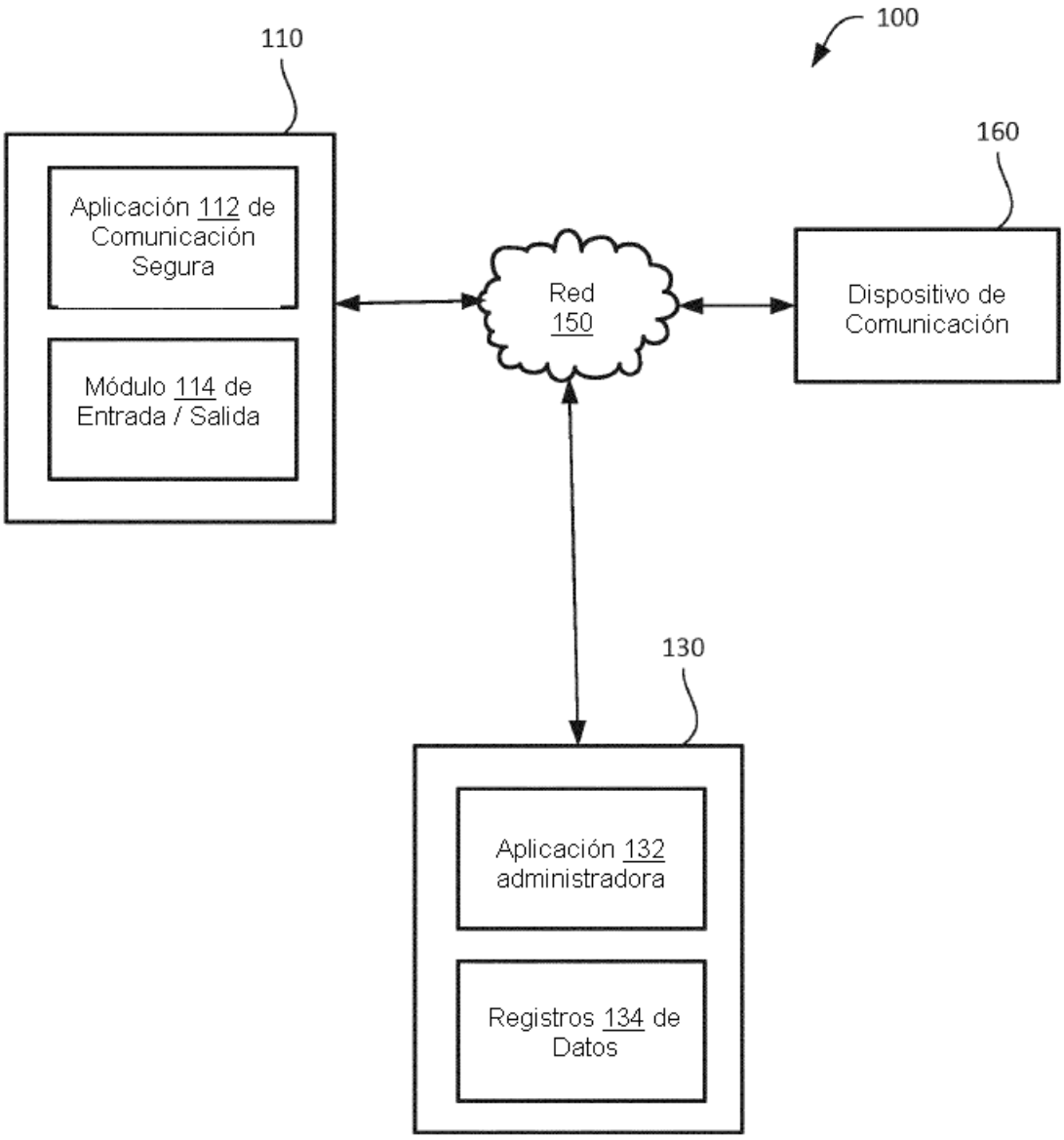
100
110
160
Aplicación 112 de Comunicación Segura
Módulo 114 de Entrada / Salida
Red 150
Dispositivo de Comunicación
130
Aplicación 132 administradora
Registros 134 de Datos

FIG. 1

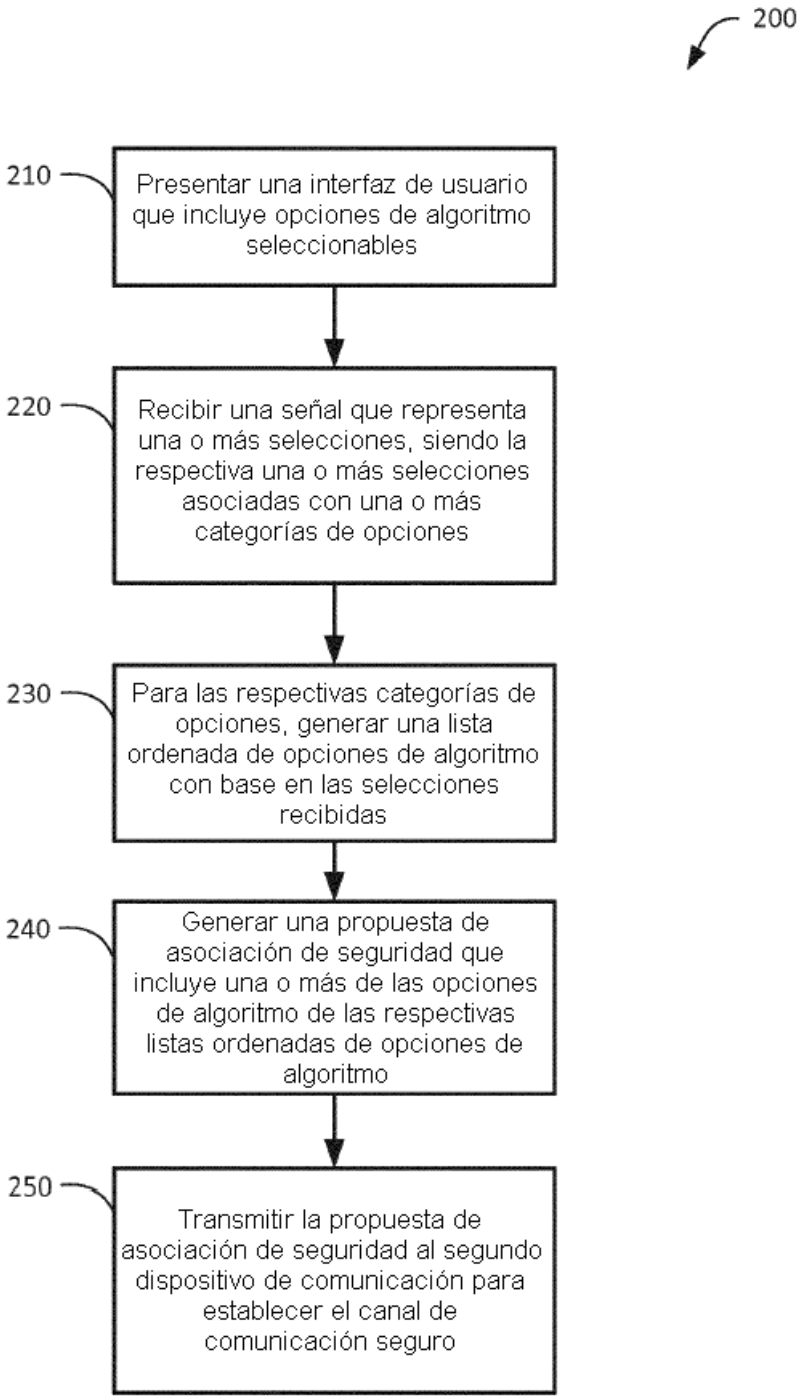
200
210
Presentar una interfaz de usuario que incluye opciones de algoritmo seleccionables
220
Recibir una señal que representa una o más selecciones, siendo la respectiva una o más selecciones asociadas con una o más categorías de opciones
230
Para las respectivas categorías de opciones, generar una lista ordenada de opciones de algoritmo con base en las selecciones recibidas
240
Generar una propuesta de asociación de seguridad que incluye una o más de las opciones de algoritmo de las respectivas listas ordenadas de opciones de algoritmo
250
Transmitir la propuesta de asociación de seguridad al segundo dispositivo de comunicación para establecer el canal de comunicación seguro

FIG. 2

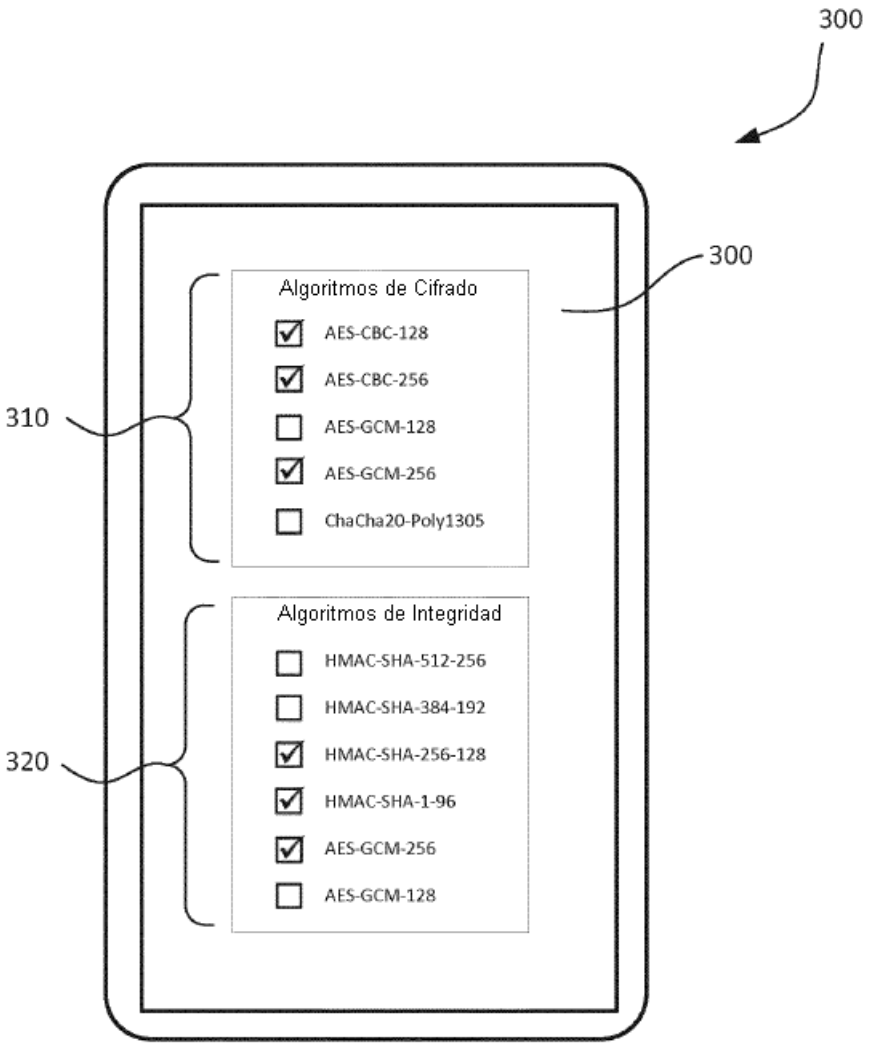
300
300
Algoritmos de Cifrado
AES-CBC-128
AES-CBC-256
AES-GCM-128
AES-GCM-256
ChaCha20-Poly1305
310
Algoritmos de Integridad
HMAC-SHA-512-256
HMAC-SHA-384-192
HMAC-SHA-256-128
HMAC-SHA-1-96
AES-GCM-256
AES-GCM-128
320

FIG. 3

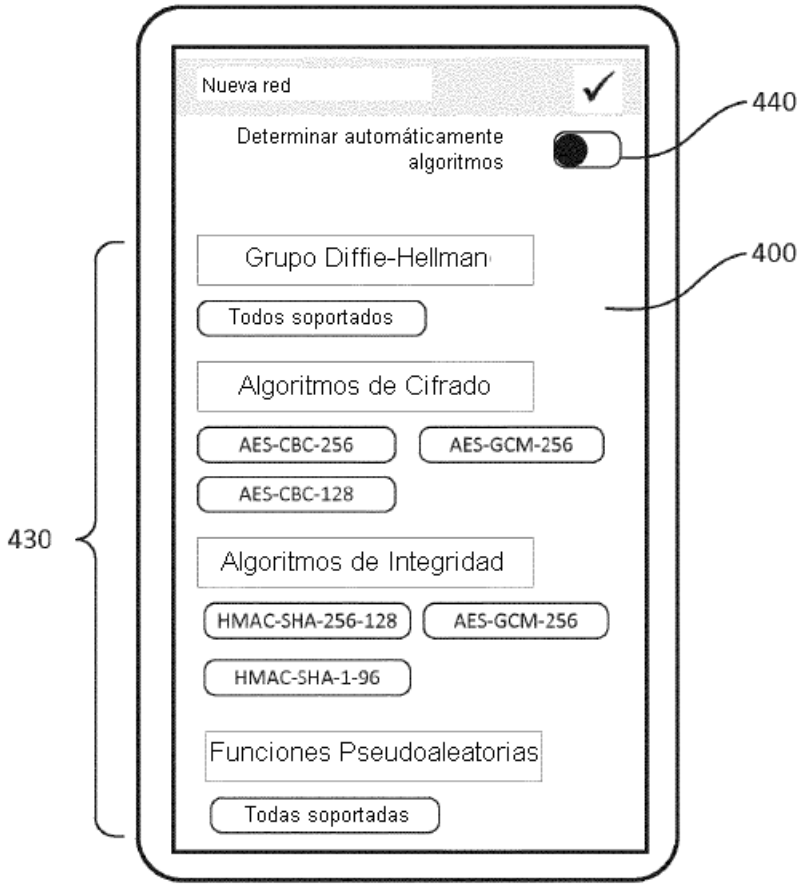
Nueva red
Determinar automáticamente algoritmos
440
400
430
Grupo Diffie-Hellman
Todos soportados
Algoritmos de Cifrado
AES-CBC-256
AES-GCM-256
AES-CBC-128
Algoritmos de Integridad
HMAC-SHA-256-128
AES-GCM-256
HMAC-SHA-1-96
Funciones Pseudoaleatorias
Todas soportadas

FIG. 4

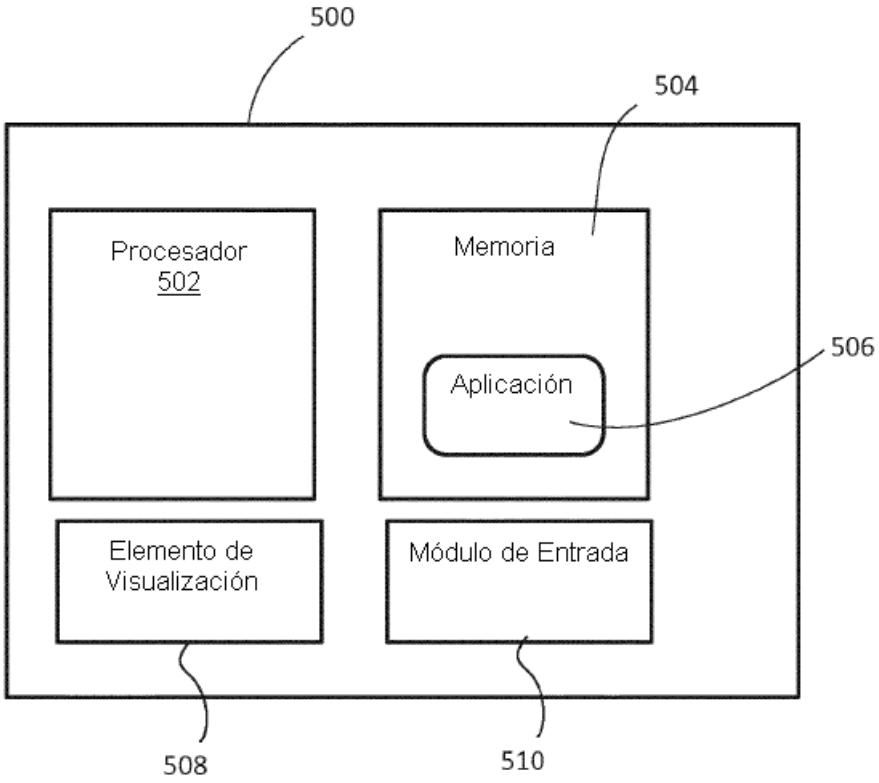
500
504
Procesador
502
Memoria
Aplicación
506
Elemento de
Visualización
Módulo de Entrada
508
510

FIG. 5