(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 775 608**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.07.2015 PCT/US2015/042359**

(87) Fecha y número de publicación internacional: **11.02.2016 WO16022326**

(96) Fecha de presentación y número de la solicitud europea: **28.07.2015 E 15747343 (0)**

(97) Fecha y número de publicación de la concesión europea: **27.11.2019 EP 3178193**

(54) Título: **Un método para proporcionar comunicación segura en tiempo real entre puntos terminales en una red**

(30) Prioridad:

08.08.2014 US 201414454812

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.07.2020

(73) Titular/es:

CELLCRYPT (100.0%)
8403 Colesville Road, Suite 1100
Silver Spring, MD 20910, US

(72) Inventor/es:

GALWAS, PAUL, ANTHONY y
WEYMAN, RAPH

(74) Agente/Representante:

INGENIAS CREACIONES, SIGNOS E INVENCIONES, SLP

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Un método para proporcionar comunicación segura en tiempo real entre puntos terminales en una red

Referencia cruzada a solicitudes relacionadas

Esta solicitud reivindica prioridad a la solicitud de Estados Unidos con n.º de serie 14/454.812 titulada METHOD OF PROVIDING REAL-TIME SECURE COMMUNICATION BETWEEN END POINTS IN A NETWORK presentada el 8 de agosto de 2014, los contenidos de la cual se incorporan completamente en el presente documento por referencia.

Campo de la invención

La presente divulgación se refiere a proporcionar comunicaciones de voz y otras en tiempo real de datos digitales a través de redes que están limitadas en ancho de banda y entre dispositivos restringidos en recursos tales como teléfonos móviles. En particular, la presente divulgación se refiere a proporcionar comunicación en tiempo real segura a través de una red de una manera eficaz en ancho de banda.

Antecedentes de la invención

En entornos restringidos en ancho de banda y potencia, tales como la telefonía móvil, es importante minimizar los datos y la complejidad de procesamiento que se requiere por los protocolos que establecen la comunicación en tiempo real segura de datos a través de una red.

Hay un campo establecido de comunicaciones en tiempo real a través de redes del Protocolo de Internet (IP), que sustenta aplicaciones generalizadas tales como Voz sobre IP (VoIP). Hay protocolos convencionales tales como el Protocolo de Iniciación de Sesión (SIP) y el Protocolo de Transporte en Tiempo Real (RTP) que soportan tráfico en tiempo real no encriptado. El RTP seguro (SRTP) se ha extendido para encriptar tráfico en tiempo real. Sin embargo, ninguno de estos protocolos son bien adecuados para entornos de ancho de banda limitado.

La Figura 1 muestra un sistema convencional que usa los protocolos anteriormente mencionados. Un punto terminal móvil (110) se comunica a través de una red inalámbrica (100) con una red de IP (200). La red de IP contiene un intermediario con estado de SIP (210), un segundo intermediario con estado de SIP (211) y un intermediario sin estado de SIP (220). Un punto terminal móvil (110) invita a otro punto terminal (120) a establecer una llamada, usando el protocolo de SIP, pasando mensajes a (210), (220) y (211). Los servidores con estado de SIP intercambian los mensajes de SIP de establecimiento de llamada finales comunicándose directamente entre sí. Cuando se establece la llamada, cada punto terminal se comunica directamente uno con el otro y los puntos terminales envían los datos en tiempo real entre sí sin encriptación usando RTP, o encriptados usando SRTP.

SRTP soporta encriptación de datos de VoIP simétrica con la Norma de Encriptación Avanzada (AES). Para encriptar una llamada usando SRTP, los puntos terminales deben obtener en primer lugar una clave de encriptación de secreto compartido. A continuación cada uno puede usar esa clave para encriptar los datos de voz que pasan entre ellos.

En algunos sistemas convencionales, cada punto terminal selecciona la clave de sesión de una lista de claves que se han cargado previamente en cada punto terminal usando un método seguro, que a menudo implica entrega física al punto terminal o cada punto terminal obtiene de manera segura la clave de sesión a través de la red desde un servidor de claves. Ambos escenarios son intensivos en ancho de banda. Además, el uso de un servidor de claves constituye un riesgo agregado. El documento "A New Provably Secure Authentication and Key Agreement Protocol for SIP Using ECC", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH, vol. 20070608: 203601, XP06100234 analiza la autenticación de SIP. El documento US2007157026 desvela un método y sistema para gestión de clave en voz sobre el protocolo de Internet. El documento US2008298579 desvela un método y sistema para autenticar un par en una red entre pares.

La presente divulgación está dirigida hacia, pero sin limitación, mejorar los problemas anteriormente indicados proporcionando mensajes de protocolo mínimos para proporcionar comunicación en tiempo real segura en un entorno de red de ancho de banda limitado.

Sumario de la invención

De acuerdo con un aspecto de la presente invención, se proporciona un método de acuerdo con la reivindicación 1. Las realizaciones ejemplares desveladas en el presente documento proporcionan un método de establecimiento de una multiplicidad de secretos compartidos en dos puntos terminales mutuamente autenticados en una red. El método, por ejemplo, incluye generar una primera clave pública (AA1pub), y una primera clave privada (AA1priv) para un primer algoritmo (AA1), una segunda clave pública (AA2pub) y una segunda clave privada (AA2priv) para un segundo algoritmo (AA2), un ID de dispositivo y un ID de pares.

Para cada llamada, o parte de una llamada, las realizaciones ejemplares proporcionan un método para crear un valor

de número aleatorio, y calcular un primer valor de autenticación (AA1-Auth) que corresponde a la primera clave pública y a la primera clave privada y un segundo valor de autenticación (AA2-Auth) que corresponde a la segunda clave pública y a la segunda clave privada. Un punto terminal receptor se autentica basándose en el primer valor de autenticación del punto terminal receptor y un punto terminal iniciador se autentica basándose en el primer valor de autenticación del punto terminal iniciador, si se verifica la autenticación del punto terminal receptor.

En otra realización ejemplar, el sistema crea el valor de autenticación AAn-Auth únicamente cuando el usuario ha sido validado satisfactoriamente usando un método biométrico, tal como, por ejemplo, una exploración de huella dactilar.

Después de que se realiza el proceso de autenticación inicial, se genera una función de intercambio de clave (DHeph) por el punto terminal receptor usando un segundo algoritmo (AA2), si la autenticación realizada por el punto terminal receptor es satisfactoria, y se calcula un secreto compartido (DHssec) por el punto terminal iniciador desde la función de intercambio de clave (Dheph) generada por el punto terminal receptor. El punto terminal iniciador genera una función de intercambio de clave (Deph) usando el segundo algoritmo (AA2) y el punto terminal receptor calcula un secreto compartido (DHssec) desde la función de intercambio de clave generada por el punto terminal iniciador.

Se realiza una segunda autenticación del punto terminal iniciador y el punto terminal receptor usando los segundos valores de autenticación calculados por el punto terminal iniciador y el punto terminal receptor. Tras la autenticación satisfactoria, se generan claves de sesión a partir de los secretos compartidos calculados.

Pueden usarse AA1-Auth y AA2-Auth para establecer confianza mutua de diferentes aspectos de un punto terminal, por ejemplo, el dispositivo, usuario, software de dispositivo, origen de software u operación de sistema. Puede usarse AA1-Auth para autenticar al usuario y puede usarse AA2-Auth para autenticar al dispositivo.

Breve descripción de los dibujos

La Figura 1 es un diagrama de bloques que ilustra un sistema de comunicación convencional.
La Figura 2 es un diagrama de bloques que ilustra una realización ejemplar de un sistema de comunicación como se desvela en el presente documento.
La Figura 3 (3A y 3B) es un diagrama de flujo que ilustra una representación ejemplar de autenticación mutua y negociación de un secreto compartido.
La Figura 4 es un diagrama de flujo que ilustra una representación ejemplar de un proceso de verificación de un valor de autenticación.
La Figura 5 es un diagrama de bloques que ilustra llamada segura desde un punto terminal activado para Acceso Múltiple por División de Código (CDMA).

Descripción detallada

La presente divulgación describe un protocolo de comunicación para proporcionar comunicaciones en tiempo real seguras en un sistema de red. El protocolo es eficaz en ancho de banda y usa mínimos datos y mensajes para efectuar comunicaciones en tiempo real seguras en la red. El protocolo realiza autenticación mutua y genera múltiples secretos compartidos para comunicaciones encriptadas.

La Figura 2 es un diagrama que ilustra una realización ejemplar de un sistema de comunicación. El sistema incluye el punto terminal 2010 que se comunica a través de la red inalámbrica 2000 con el sistema de red 2200, y el punto terminal 2110 que se comunica con el sistema de red a través de la red inalámbrica 2100. El sistema de red interconecta dos puntos terminales en el sistema de comunicación, y el sistema de comunicación puede incluir dos o más puntos terminales.

El punto terminal 2010 puede ser, por ejemplo, un punto terminal móvil que incluye equipo móvil (por ejemplo, teléfono móvil) equipado con módulos de encriptación. Los módulos de encriptación proporcionan funciones de encriptación y desencriptación para datos de voz en tiempo real y establece un enlace de comunicación seguro con otro punto terminal en el sistema de comunicación. Los módulos de encriptación pueden ser procesadores embebidos con instrucciones legibles por ordenador que, cuando se ejecutan, realizan funciones de encriptación y desencriptación.

El punto terminal 2110 puede ser, por ejemplo, otro punto terminal móvil, tal como el punto terminal 2010, o un dispositivo de pasarela, tal como la pasarela 2111. La pasarela 2111 conecta un sistema telefónico tradicional, tal como, por ejemplo, la Red Telefónica Pública Conmutada (PSTN) y la Centralita Privada (PBX) al sistema de red 2200. La pasarela convierte el tráfico telefónico de PSTN o PBX en un formato de IP para su transmisión a través de una red de IP. La pasarela 2111 está equipada con un módulo de encriptación para facilitar las funciones de encriptación y desencriptación. Se proporciona encriptación de punto a punto transparente entre el punto terminal 2010 y el punto terminal 2110, y entre el punto terminal 2010 y la pasarela 2111.

Los módulos de encriptación pueden usar esquemas de encriptación redundantes para la sesión, autenticación, generación de resumen y/o intercambio de clave. Las realizaciones preferidas usan dos algoritmos fuertes al mismo tiempo en serie. La encriptación de los datos puede realizarse usando cualquier algoritmo de criptografía conocido, tal

como, por ejemplo, curva elíptica Diffie-Hellman (ECDH), Rivest, Shamir y Adleman (RSA), Norma de Encriptación Avanzada (AES), Algoritmo de Firma Digital (DSA), etc.

Las redes 2000 y 2100 son sistemas de red inalámbrica, tales como, por ejemplo, Sistemas Globales para Comunicación Móvil (GSM), Tasas de Datos Mejoradas para la Evolución de GSM (EDGE), Servicio General de Paquetes de Radio (GPRS), 3G GSM, HSPA, UMTS, CDMA y Wi-Fi.

El sistema de red 2200 es un sistema de red alámbrica, tal como, por ejemplo, un sistema del Protocolo de Internet (IP). El sistema de red puede incluir uno o más servidores de señalización y uno o más servidores de medios. Un punto terminal envía una solicitud al servidor de señalización para realizar una llamada o enviar un mensaje a otro punto terminal. El servidor de señalización establece la llamada, indicando a cada punto terminal que entre en contacto con el mismo servidor de medios. Los puntos terminales envían los datos en tiempo real entre sí a través del servidor de medios. El servidor de medios usa protocolos de medios para recibir datos de voz y los envía a través de la red.

El dispositivo de almacenamiento 2240 puede implementarse con una diversidad de componentes o subsistemas que incluyen, por ejemplo, una unidad de disco magnético, una unidad óptica, memoria flash, o cualesquiera otros dispositivos que puedan almacenar información de manera persistente. El dispositivo de almacenamiento incluye la base de datos de dispositivos 2215, que contiene una lista de todos los ID de dispositivo conocidos para el sistema.

La arquitectura mostrada en la Figura 2 permite la comunicación (por ejemplo, transmisión de datos, llamada telefónica y vídeo) entre dos puntos terminales o entre un punto terminal y una pasarela en el sistema. Las comunicaciones están encriptadas usando los protocolos descritos a continuación e ilustrados en la Figura 3 y la Figura 4. Las comunicaciones en tiempo real entre dos puntos terminales o entre un punto terminal y una pasarela se encriptan usando una o más claves de sesión que se derivan de un secreto compartido conocido únicamente para los puntos terminales.

Como se ilustra en la Figura 3, en la etapa 3500a, cada punto terminal y/o pasarela (por ejemplo, un punto terminal iniciador/pasarela y un punto terminal receptor/pasarela) genera, en un momento predeterminado, tal como, por ejemplo, en la instalación, una primera clave pública (AA1pub), y una primera clave privada (AA1priv) para un primer algoritmo (AA1), una segunda clave pública (AA2pub) y una segunda clave privada (AA2priv) para un segundo algoritmo (AA2), un ID de dispositivo y un ID de pares. La primera clave pública (AA1pub), primera clave privada (AA1priv), segunda clave pública (AA2pub) y segunda clave privada (AA2priv) pueden generarse por cualquier método bien conocido en la técnica.

En otra realización ejemplar, la primera clave pública es un correspondiente certificado digital (Cert-AA1(x)) para un algoritmo criptográfico asimétrico (AA1) y la segunda clave pública es un correspondiente certificado digital (Cert-AA2(x)) para un algoritmo criptográfico asimétrico diferente (AA2). Los certificados digitales Cert-AA1(x) y Cert-AA2(x) cada uno puede ser un certificado X509 que contiene uno o más atributos, tales como, por ejemplo, ID de dispositivo, ID de pares, ID, ID de software, ID de origen de software, ID de operación de sistema y nombre, para un correspondiente punto terminal.

El primer algoritmo (AA1) y el segundo algoritmo (AA2) son algoritmos criptográficos. En una realización, el primer algoritmo (AA1) y el segundo algoritmo (AA2) se usan para autenticar un mismo parámetro. En esta realización, el primer algoritmo (AA1) y el segundo algoritmo (AA2) usan diferentes algoritmos criptográficos diferentes. Por ejemplo, el primer algoritmo (AA1) puede ser Rivest, Shamir y Adleman (RSA) y el segundo algoritmo (AA2) puede ser Algoritmo de Firma Digital (DSA).

En otra realización ejemplar, el primer algoritmo (AA1) y el segundo algoritmo (AA2) se usan para autenticar diferentes parámetros. En esta realización, el primer algoritmo (AA1) y el segundo algoritmo (AA2) usan el mismo algoritmo criptográfico.

En otra realización ejemplar, el primer algoritmo (AA1) se sustituye por un algoritmo nulo de manera que la encriptación con cualquier clave proporciona el mismo texto encriptado como una entrada de texto plano y la encriptación proporciona el mismo texto desencriptado como el texto de entrada, y las firmas siempre se verifican.

El ID de dispositivo de un punto terminal se usa para identificar el dispositivo únicamente al servidor de señalización y se crea por su correspondiente punto terminal. El punto terminal puede derivar el ID de dispositivo de un identificador de hardware en el punto terminal, tal como la Identidad de Equipo Móvil Internacional de GSM (IMEI). Como alternativa, el punto terminal puede crear el ID de dispositivo, por ejemplo usando un generador de número aleatorio. El ID de dispositivo puede entregarse a la base de datos de dispositivos 2215 por un canal fuera de banda.

En otra realización ejemplar, otro componente de sistema genera el ID de dispositivo y lo entrega al punto terminal asociado y a la base de datos de dispositivos 2215 por el canal fuera de banda.

El ID de pares identifica el dispositivo al servidor de medios y se genera usando un generador de número aleatorio. En otra realización ejemplar, el ID de pares se deriva de una clave pública de un par de claves criptográficas

asimétricas que genera un punto terminal cuando se crea. El ID de pares de un punto terminal es independiente de la dirección de IP y se usa para identificar mensajes de medios de un correspondiente punto terminal en el sistema de comunicación.

En la etapa 3500b, se genera un valor de número aleatorio (N) para cada llamada o parte de una llamada. El valor de número aleatorio (N) se genera desde un generador de número aleatorio.

En la etapa 3510, cada punto terminal (por ejemplo, un punto terminal iniciador y un punto terminal receptor) calcula un primer valor de autenticación (AA1-Auth) que corresponde a la primera clave pública y a la primera clave privada y un segundo valor de autenticación (AA2-Auth) que corresponde a la segunda clave pública y la segunda clave privada.

El primer valor de autenticación (AA1-Auth) se calcula, por ejemplo, como AA1-Auth(x) = AA1_encrypt(Nx, AA1puby) concatenado con AA1_sign_withH1 (mensajes, AA1priv(x)). Mensajes = todos los mensajes enviados(x) concatenados con todos los mensajes recibidos(x). El subíndice x identifica el emisor del mensaje del protocolo y el subíndice y identifica el receptor de mensaje de protocolo. AA1_encrypt es el algoritmo de encriptación que usa la clave pública. AA1_sign_withH1 es un algoritmo de firma (por ejemplo, DSA) que usa la clave privada y un algoritmo de resumen (H1) (por ejemplo, SHA-384).

El segundo valor de autenticación (AA2-Auth) se calcula, por ejemplo, como AA2-Auth(x) = AA2-SIG(x)_withH2(todos los mensajes enviados(x) concatenados con todos los mensajes recibidos(x)). AA2-SIG(x)_withH2 es un algoritmo de firma que usa la clave privada y un algoritmo de resumen (H2). Los algoritmos de resumen H1 y H2 son diferentes entre sí.

Si se pierde cualesquiera de los mensajes enviados(x), los mensajes se reenvían de una memoria intermedia. Los mensajes perdidos no se recalculan.

En la etapa 3520, un punto terminal iniciador (por ejemplo, el punto terminal 2010) inicia un proceso de autenticación mutua generando un mensaje y enviando el mensaje generado a un punto terminal receptor (por ejemplo, el punto terminal 2110) en el sistema de comunicación. El formato de mensaje es, por ejemplo, [ID de pares (2010), N (2010), $AA1_{pub}$ (2010)], en el que ID de pares (2010) es el ID de pares del punto terminal 2010, N (2010) es el valor de número aleatorio generado por el punto terminal 2010 y $AA1_{pub}$ (2010) es la clave pública del iniciador o correspondiente certificado digital para el primer algoritmo (AA1).

Tras recibir el mensaje, el punto terminal receptor envía un mensaje al punto terminal iniciador, en la etapa 3530. El formato del mensaje es, por ejemplo, [ID de pares(2110), N(2110), $AA1_{pub}$ (2110), AA1-Auth (2110)]. El ID de pares (2110) es el ID de pares del punto terminal 2110, N (2110) es el valor de número aleatorio generado por el punto terminal 2110 y $AA1_{pub}$ (2110) es la clave pública del iniciador o correspondiente certificado para el primer algoritmo (AA1). AA1-Auth (2110) es el primer valor de autenticación calculado por el punto terminal 2110.

En la etapa 3540, el punto terminal iniciador 2010 verifica el valor de autenticación del punto terminal 2110.

Cada punto terminal contiene una base de datos de contactos confiables (no mostrada) de contactos confiables. Cada contacto confiable contiene para un punto terminal dado un nombre, ID de llamada, ID de pares, Credencial1 y opcionalmente Credencial, donde nombre es una cadena definida por el usuario para identificar el contacto, ID de llamada puede usarse como un ID de llamante, o ID del llamado, y CredencialZ es AAZpub, o Cert-AAZ, y Z=1 o 2.

Cuando se inicia una llamada, el punto terminal del llamante (2010) (es decir, el punto terminal iniciador) genera un ID de establecimiento que identifica la solicitud para hacer una llamada a un punto terminal en la red (por ejemplo 2110)(es decir, el punto terminal receptor), y envía un mensaje de solicitud 1 de llamada a un servidor de señalización (no mostrado) que debe contener el ID de establecimiento, ID de sesión, ID del llamado e ID del llamante. El ID del llamado es un número para identificar el punto terminal (2010) y el ID del llamante es un número para identificar el punto terminal (2110).

Al recibir el mensaje de la solicitud 1 de llamada, el servidor de señalización mapea el ID del llamado a un ID de dispositivo usando una base de datos y comprueba si el punto terminal tiene un ID de sesión para mostrar que se ha registrado. En caso afirmativo, el servidor de señalización genera un ID de llamada que identifica la llamada, selecciona un servidor de medios y envía un mensaje de solicitud 2 de llamada al punto terminal (2110) que debe contener ID del llamado, ID de llamante, dirección de MS, donde la dirección de MS es la dirección de IP del servidor de medios que llevará la llamada.

El valor de autenticación se verifica usando un algoritmo, que utiliza información de los mensajes de solicitud de llamada. El algoritmo, como se ilustra en la Figura 4, incluye, por ejemplo, lo siguiente:

En la etapa 401, si el punto terminal 2010 es el llamante (A) (es decir, el punto terminal iniciador), halla el contacto confiable que hace coincidir el ID del llamado que corresponde al punto terminal 2010. Si el punto terminal 2110 es el llamado (B) (es decir, el punto terminal receptor), halla el contacto confiable que hace coincidir el ID del llamante que

corresponde al punto terminal 2110, que se obtiene del mensaje de la solicitud 2 de llamada.

En la etapa 402, determinar si se halla una coincidencia.

Si se halla una coincidencia, en la etapa 403, calcular los resultados de verificación como sigue:

a. Si se halla una coincidencia para el punto terminal B (2110),
ResultadoA = (ID del llamante del mensaje de solicitud 2 de llamada coincide con ID del llamado del contacto confiable)
b. si se halla una coincidencia para el punto terminal A (2010),
ResultadoA = (ID del llamado coincide con ID del llamante del contacto confiable)
c. ResultadoB = verificar AAZ-Auth (por ejemplo, AA1-Auth (2110)) usando la CredencialZ del contacto confiable, usando un algoritmo de verificación criptográfico convencional para AAZ (por ejemplo AA1)
d. Resultado_verificaciónZ = ResultadoA y ResultadoB
e. Si Resultado_verificaciónZ es VERDADERO, establecer LlamadaConfiableZ a VERDADERO

Si no se halla coincidencia, en la etapa 404, establecer el resultado de verificación a VERDADERO y la LlamadaConfiableX a falso.

ResultadoX y LlamadaConfiableX (X = A o B), Resultado_VerificaciónZ (Z=1 o 2) son valores lógicos, con valores VERDADERO o FALSO.

Si el primer valor de autenticación se verifica satisfactoriamente, el punto terminal 2010 envía su primer valor de autenticación al punto terminal 2110 para su verificación. De lo contrario el proceso se termina.

En la etapa 3550, el punto terminal receptor 2110 verifica el valor de autenticación del punto terminal 2010 de la manera ilustrada en la Figura 4. Si el primer valor de autenticación se verifica satisfactoriamente, el punto terminal 2110 genera una función de intercambio de clave (DHeph) (por ejemplo, intercambio de claves diffie-hellman) usando el segundo algoritmo (AA2) y genera un mensaje para enviar al punto terminal 2010. El formato de mensaje es, por ejemplo, [AA2pub (2110), Dheph(2110)]. AA2pub (2110) es la clave pública del receptor (2110) o correspondiente certificado digital para el segundo algoritmo (AA2). Si el primer valor de autenticación no se verifica satisfactoriamente, el proceso se termina.

Tras recibir el mensaje, el punto terminal 2010 calcula una variable DHssec del intercambio de claves Diffie-Hellman Dheph (2110), y genera una función de intercambio de clave (DHeph)(2010)(por ejemplo, intercambio de claves Diffie-Hellman) usando el segundo algoritmo (AA2), en la etapa 3560. El punto terminal 2010 genera un mensaje para enviar al punto terminal 2110. El formato de mensaje es, por ejemplo, [AA2pub (2010), Dheph(2010)]. AA2pub (2010) es la clave pública del iniciador (2010) o correspondiente certificado digital para el segundo algoritmo (AA2).

En la etapa 3570, el punto terminal 2110 calcula una variable DHssec del intercambio de claves Diffie-Hellman Dheph (2010), y envía al punto terminal 2010 su segundo valor de autenticación (AA2-Auth(2010)).

El intercambio de claves Diffie-Hellman proporciona secreto hacia delante, es decir, asegura que una clave de sesión derivada de un conjunto de claves públicas y privadas a largo plazo no estará comprometida si una de las clave privadas (a largo plazo) está comprometida en el futuro. Por otro lado, si se obtiene la clave por un pirata, cualesquiera mensajes correspondientes no se verán comprometidos.

En la etapa 3580, el punto terminal 2010 verifica el segundo valor de autenticación del punto terminal 2110 de la manera ilustrada en la Figura 4. Si no se verifica el valor de autenticación, tiene lugar un fallo de autenticación y el proceso se termina. Si no se verifica el valor de autenticación, el punto terminal 2010 envía al punto terminal 2110 su segundo valor de autenticación (AA2-Auth(2010)) y calcula las claves de sesiones como se describe a continuación.

Tras recibir el segundo valor de autenticación del punto terminal 2010, en la etapa 3590, el punto terminal 2110 verifica el segundo valor de autenticación de la manera ilustrada en la Figura 4. Si no se verifica el valor de autenticación, tiene lugar un fallo de autenticación y el proceso se termina. Si no se verifica el valor de autenticación, el punto terminal 2110 calcula claves de sesiones como se describe a continuación.

El flujo de datos en tiempo real se encripta con un flujo de claves (es decir, claves de sesión), generado usando un primer algoritmo simétrico (SA1) y a continuación un segundo algoritmo simétrico (SA2). Por ejemplo SA1 puede ser RC4 y SA2 puede ser AES en modo CTR.

En una realización de la invención, SA1 se sustituye por un algoritmo nulo, de manera que la encriptación con cualquier clave proporciona ese mismo texto encriptado como la entrada de texto plano, y la encriptación proporciona el mismo texto desencriptado como la entrada.

El flujo de claves se inicializa, como sigue, por ejemplo, para una clave de 248 bits:

El enlace descendente de A y en enlace ascendente de B:

K_{SA1} = Bytes 0 a 31 de PRF(SSEC2)
K_{SA2} = Bytes 0 a 31 de PRF(SSECI)
IV_{SA2} = Bytes 32 a 47 de PRF(SSECI)

El enlace descendente de A y en enlace ascendente de B:

K_{SA1} = Bytes 32 a 63 de PRF(SSEC2)
K_{SA2} = Bytes 48 a 79 de PRF(SSECI)
IV_{SA2} = Bytes 80 a 95 de PRF(SSECI)

PRF indica una función pseudoaleatoria. Los secretos compartidos, SSEC1 y SSEC2 se calculan, como sigue:

SSEC1 = H2(N_A concatenado con N_B),
SSEC2 = Doble_troceo(SSEC1 concatenado con Doble_troceo(DH_{ssec})),

donde Doble_troceo(X) = XOR-cíclico (H2 (X), H3 (X))) y H2 y H3 son diferentes algoritmos de resumen, por ejemplo SHA-512 y MD5. N_A es el número aleatorio generado por el punto terminal iniciador y N_B es el número aleatorio generado por el punto terminal receptor.

En otra realización ejemplar, se usa SSEC1 = NULO, y únicamente 1 clave secreta para inicializar un flujo de claves.

En otras realizaciones de la invención, el enfoque se generaliza para crear más de dos secretos compartidos.

Las comunicaciones entre puntos terminales 2010 y 2110 se encriptan usando las claves de sesión calculadas.

Cuando el punto terminal 2110 es una pasarela, la pasarela usa las mismas claves asimétricas (A pub, A priv) para autenticarse a sí misma en todas las llamadas.

En otra realización ejemplar, la pasarela tiene una base de datos que almacena un conjunto de pares de claves asimétricas asociados con cada número de teléfono seguro o intervalo confiable que da servicio. Cuando la pasarela recibe o hace una llamada usando un número de teléfono seguro, halla los correspondientes pares de claves asimétricas de la base de datos y los usa en el protocolo ilustrado en la Figura 3.

Adicionalmente, antes de que pueda establecerse una ruta encriptada entre dos puntos terminales o entre un punto terminal y la pasarela (por ejemplo, el punto terminal 2010 y la pasarela 2111) en el sistema de comunicación, debe tener lugar una autenticación mutua (por ejemplo, entre el dispositivo del punto terminal 2010 y la pasarela 2111) como se describe en la Figura 3.

En otra realización ejemplar, el sistema de comunicación proporciona autenticación distribuida y de 2 factores, por ejemplo, a un servicio de telefonía, tal como un puente de conferencia, en la infraestructura de telefonía. El servicio de telefonía tiene una base de datos que contiene una lista blanca de los ID del llamante que pueden usar el servicio. Cuando se establece una llamada al servicio, la pasarela 2111 envía el ID del llamante a una PBX, que envía el ID del llamante al servicio de telefonía. El servicio únicamente permite el acceso si el ID del llamante está en la base de datos.

En otra realización ejemplar, la base de datos podría contener una lista negra de los ID de llamantes que no pueden usar el servicio.

Una vez que se establece la llamada, el servicio de telefonía puede usar también indicaciones de voz para solicitar datos de autenticación adicionales, tales como un PIN, del llamante. Cuando el llamante introduce el PIN, el sistema lo envía como una señal de múltiples frecuencias de tono dual (DTMF), y el servicio de telefonía verifica el PIN. Los tonos DTMF se encriptan entre los puntos terminales. Si la verificación falla, el servicio de telefonía termina la llamada, de lo contrario, un punto terminal (por ejemplo, el punto terminal 2010) puede comunicarse con otro punto terminal (por ejemplo, el punto terminal 2110) en el sistema de comunicación usando DTMF.

El punto terminal 2010 puede solicitar un servicio de conferencia, y responder a indicaciones de voz del servicio de conferencia usando señales de DTMF para seleccionar una sala de conferencias e introducir un pin para autenticar al llamante. En este caso, el punto terminal codifica señales de DTMF en el tráfico de medios y la pasarela las decodifica y las transmite de una manera convencional a una PBX.

El sistema codifica señales de DTMF en tramas que sustituyen tramas de códec convencionales (como se describe a continuación). De esta manera, las señales de DTMF encriptadas pueden mezclarse de manera arbitraria con voz encriptada.

Un punto terminal codifica datos de voz usando una modificación a un códec de tasa adaptativa convencional, tal como el códec de audio tasa múltiple adaptativa (AMR). La modificación reduce el ancho de banda requerido para transmitir los datos del códec convencional. El sistema negocia la tasa de códec en una base por llamada y usa este conocimiento para reducir los datos transmitidos en cada trama de códec.

Cuando se registra un punto terminal, el mensaje de registro contiene un campo de versión de protocolo, que contiene una codificación de la tasa o tasas de códec que puede usar el punto terminal. El servidor de señalización determina qué tasa de códec pueden usar los puntos terminales en una llamada y notifica a cada punto terminal de la elección en mensajes de protocolo.

En otra realización ejemplar, los puntos terminales negocian la tasa de extremo a extremo de códec en el comienzo de la sesión. En este caso, ambos puntos terminales conocen la tasa de un códec adaptativo de múltiples tasas para usar en una llamada entre ellos sin que esté implicado el servidor de señalización, y por lo tanto, los puntos terminales pueden eliminar el componente de encabezado de todas las tramas.

Para reducir el ancho de banda usado, un punto terminal (por ejemplo, el punto terminal 2010) elimina los datos de encabezamiento de una trama de códec convencional que contienen la información de tasa antes de enviar la trama a la otra parte en una llamada. El otro punto terminal de la llamada (por ejemplo, el punto terminal 2110) añade los datos de códec convencional equivalente a cada trama modificada cuando la recibe.

En una realización ejemplar, el punto terminal 2010 forma un paquete que comprende múltiples tramas modificadas concatenadas y transmite las tramas concatenadas a la otra parte en la llamada.

En otra realización ejemplar, se determina la tasa de códec convencional por codificación de longitud de serie. Este método reduce el ancho de banda puesto que únicamente se notifica a un punto terminal cuando cambia la velocidad.

El proceso de autenticación para acceder a un servicio de telefonía puede distribuirse en más de un lugar (por ejemplo, la pasarela, la PBX y el servicio). Si estas funciones están físicamente separadas, entonces sería necesario comprometer todas ellas para comprometer el proceso de autenticación.

En otra realización ejemplar, cuando se establece una llamada, un punto terminal puede calcular un código que es único para esa llamada. En el caso de que ambos puntos terminales en la llamada sean teléfonos móviles, cada uno puede visualizar el código al usuario. Un llamante puede leer el código para el otro, que puede confirmar que es el mismo código que se visualiza en su teléfono.

El código puede derivarse de las claves de sesión calculadas, por ejemplo, usando una función de resumen.

En el caso cuando un punto terminal sea una pasarela, la pasarela puede calcular el código y lo pasa a una PBX, que puede retransmitir el código a un punto terminal en el sistema de comunicación, tal como un teléfono. El teléfono podría visualizar el código, permitiendo de esta manera que los llamantes confirmen sus códigos.

De una manera similar, la pasarela podría transferir un mensaje no verbal que haya recibido de manera segura desde un punto terminal móvil al sistema de comunicación.

La Figura 5 ilustra la llamada segura de los puntos terminales aptos para Acceso Múltiple por División de Código (CDMA). El punto terminal 500 es un punto terminal móvil de CDMA que incluye equipo móvil (por ejemplo, teléfono móvil equipado con módulos de encriptación). El equipo móvil incluye un altavoz 530, un micrófono 540, un botón 510 y una aplicación de telefonía segura 520. La aplicación de telefonía segura 520 usa comunicaciones de audio símplex, donde el usuario presiona el botón 520 en el microteléfono para hablar.

Cuando se presiona el botón 510, la aplicación 520 deja de reproducir el audio recibido a través del canal de comunicación seguro 550 a un punto terminal 570 en una red de llamadas segura 560 y transmite audio grabado desde el micrófono 540.

Cuando no se presiona el botón 510, la aplicación 520 reproduce en el altavoz 530 el audio recibido del canal de comunicación seguro 550 a un punto terminal 570 en la red de llamadas segura 560 e ignora audio del micrófono 540.

En otra realización ejemplar, cuando se presiona el botón 510, la aplicación 520 envía un mensaje hasta el canal de llamada encriptado al punto terminal 570. Cuando el punto terminal 570 recibe este mensaje, no transmite audio al punto terminal 500 y la aplicación 520 transmite audio grabado del micrófono 540 al punto terminal 570.

En otra realización ejemplar, es posible presionar uno de un conjunto de botones donde cada botón envía un mensaje diferente hasta el canal de llamada encriptado. Cuando se recibe el mensaje, el punto terminal 570 visualiza texto o un icono dependiendo de qué botón se presione. Por ejemplo, el punto terminal 570 visualiza el texto, por ejemplo, "en cooperación" en respuesta al mensaje recibido de un botón programado para indicar cooperación.

Como se desvela en el presente documento, las realizaciones y características de la invención pueden implementarse a través de hardware y/o software informático. Tales realizaciones pueden implementarse en diversos entornos, tales como entornos en red e informáticos. La presente invención no está limitada a tales ejemplos, y las realizaciones de la invención pueden implementarse con otras plataformas y en otros entornos.

Además, aunque se han descrito realizaciones ilustrativas de la invención en el presente documento, realizaciones adicionales pueden incluir elementos equivalentes, modificaciones, omisiones, combinaciones (por ejemplo, de aspectos a través de diversas realizaciones) adaptaciones y/o modificaciones como se apreciaría por los expertos en la materia basándose en la presente divulgación.

REIVINDICACIONES

1. Un método de establecimiento de una multiplicidad de secretos compartidos en dos puntos terminales de usuario mutuamente autenticados en una red, que comprende las etapas de:

generar, por cada punto terminal, una primera clave pública ($AA1_{pub}$), y una primera clave privada ($AA1_{pnv}$) para un primer algoritmo (AA1), una segunda clave pública ($AA2_{pub}$) y una segunda clave privada ($AA2_{priv}$) para un segundo algoritmo (AA2), un ID de dispositivo y un ID de pares, en un periodo de tiempo predeterminado;
generar un valor de número aleatorio para cada llamada;
calcular, por cada punto terminal, un primer valor de autenticación (AA1-Auth) que corresponde a la primera clave pública y a la primera clave privada y un segundo valor de autenticación (AA2-Auth) que corresponde a la segunda clave pública y a la segunda clave privada;
iniciar un proceso de autenticación mutua generando un mensaje, por un punto terminal iniciador de llamada, y enviar el mensaje generado a un punto terminal receptor de llamada en la red;
autenticar, por el punto terminal iniciador, el punto terminal receptor basándose en el primer valor de autenticación del punto terminal receptor que incluye:

autenticar, por el punto terminal iniciador, el punto terminal receptor basándose en el segundo valor de autenticación del punto terminal receptor;
autenticar, por el punto terminal receptor, el punto terminal iniciador basándose en el segundo valor de autenticación del punto terminal iniciador, si dicha autenticación realizada por el punto terminal iniciador es satisfactoria, de lo contrario terminar
calcular claves de sesión, por el punto terminal iniciador usando el secreto compartido calculado por el punto terminal iniciador, si la autenticación del punto terminal receptor por el punto terminal iniciador basándose en el respectivo segundo valor de autenticación es satisfactoria,
calcular claves de sesión, por el punto terminal receptor, usando el secreto compartido calculado por el punto terminal receptor, si la autenticación del punto terminal iniciador por el punto terminal receptor basándose en el respectivo segundo valor de autenticación es satisfactoria;
autenticar, por el punto terminal receptor, el punto terminal iniciador basándose en el primer valor de autenticación del punto terminal iniciador, si dicha autenticación realizada por el punto terminal iniciador es satisfactoria;
generar, por el punto terminal receptor, una función de intercambio de clave (DH_{eph}) usando el segundo algoritmo (AA2), si dicha autenticación realizada por el punto terminal receptor es satisfactoria;
calcular, por el punto terminal iniciador, un secreto compartido (DH_{ssec}) de la función de intercambio de clave (Dheph) generada por el punto terminal receptor;
generar, por el punto terminal iniciador, una función de intercambio de clave (DH_{eph}) usando el segundo algoritmo (AA2); y
calcular, por el punto terminal receptor, un secreto compartido (DH_{ssec}) de la función de intercambio de clave generada por el punto terminal iniciador,

en el que la autenticación mutua tiene éxito únicamente cuando las partes reciben todos los mensajes que la otra parte ha enviado y en el mismo orden.

2. El método de la reivindicación 1, en el que el mensaje comprende una solicitud de establecimiento de llamada, comprendiendo la etapa de envío del mensaje generado enviar la solicitud de establecimiento de llamada mediante un servidor de señalización a un punto terminal receptor de llamada en la red, usando las etapas de autenticación un algoritmo que utiliza información de la solicitud de establecimiento de llamada.

3. El método de la reivindicación 1, que comprende adicionalmente la etapa de: calcular múltiples claves de secreto compartido, en el que al menos una clave de secreto compartido se calcula desde $DH_{ssec.}$

4. El método de la reivindicación 3, en el que las claves de sesión calculadas se calculan desde las múltiples claves de secreto compartidas calculadas.

5. El método de cualquier reivindicación anterior, en el que tiene lugar un proceso de terminación si cualquier autenticación realizada es insatisfactoria.

6. El método de la reivindicación 1, en el que el secreto compartido (DH_{ssec}) se genera únicamente cuando la realización de todas las autenticaciones es satisfactoria.

7. El método de la reivindicación 1, en el que la autenticación tiene éxito únicamente cuando el ID de pares del dispositivo coincide con un valor almacenado en una base de datos de contactos confiables y una firma digital verifica el contacto usando una o más correspondientes claves públicas.

8. El método de la reivindicación 5, en el que el ID de pares se genera usando un generador de número aleatorio.

9. El método de la reivindicación 5, en el que el ID de pares se deriva de una clave pública de un par de claves criptográficas asimétricas que se generan por un correspondiente punto terminal.

10. El método de la reivindicación 1, en el que el número aleatorio se genera múltiples veces durante una llamada.

11. El método de la reivindicación 1, en el que los mensajes enviados durante la autenticación se reenvían desde una memoria intermedia si se perdiera algún mensaje.

12. El método de la reivindicación 1, en el que los puntos terminales incluyen equipo móvil que contiene una aplicación, botón, altavoz, micrófono y una pluralidad de botones, estando configurada la pluralidad de botones para provocar que el equipo móvil envíe un mensaje cuando se presiona su correspondiente botón.

13. El método de la reivindicación 1, en el que se codifican datos usando un códec de tasa adaptativa convencional modificado, negociándose la tasa de códec en una base por llamada por los puntos terminales en el comienzo de la sesión.

SISTEMA CONVENCIONAL

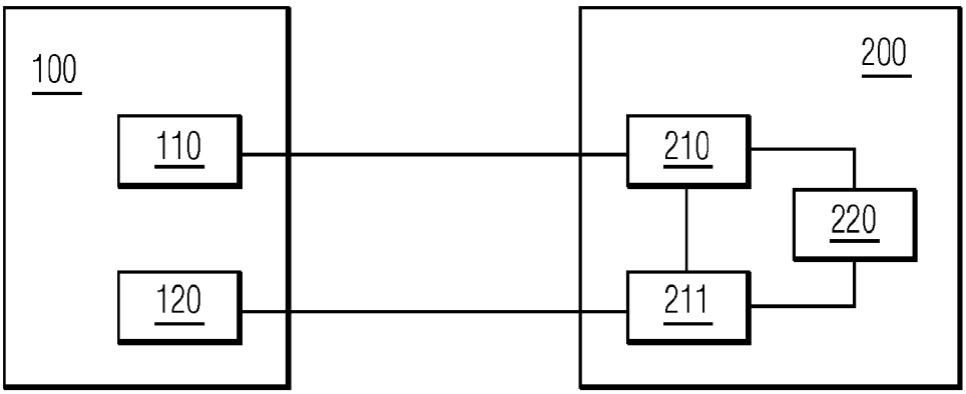

FIG. 1

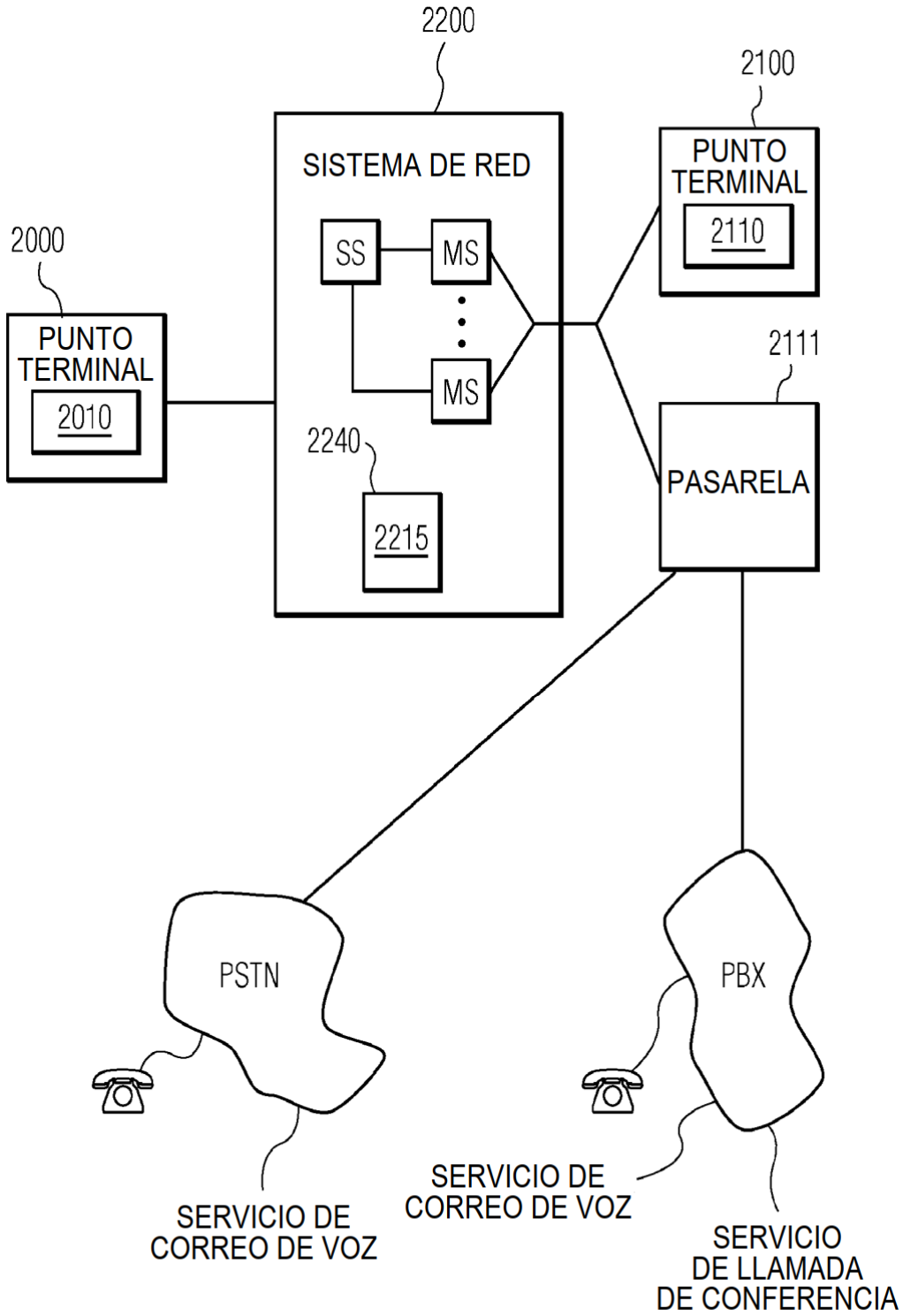
2200
SISTEMA DE RED
SS
MS
MS
2240
2215
2100
PUNTO TERMINAL
2110
2111
PASARELA
2000
PUNTO TERMINAL
2010
PSTN
PBX
SERVICIO DE CORREO DE VOZ
SERVICIO DE CORREO DE VOZ
SERVICIO DE LLAMADA DE CONFERENCIA

FIG. 2

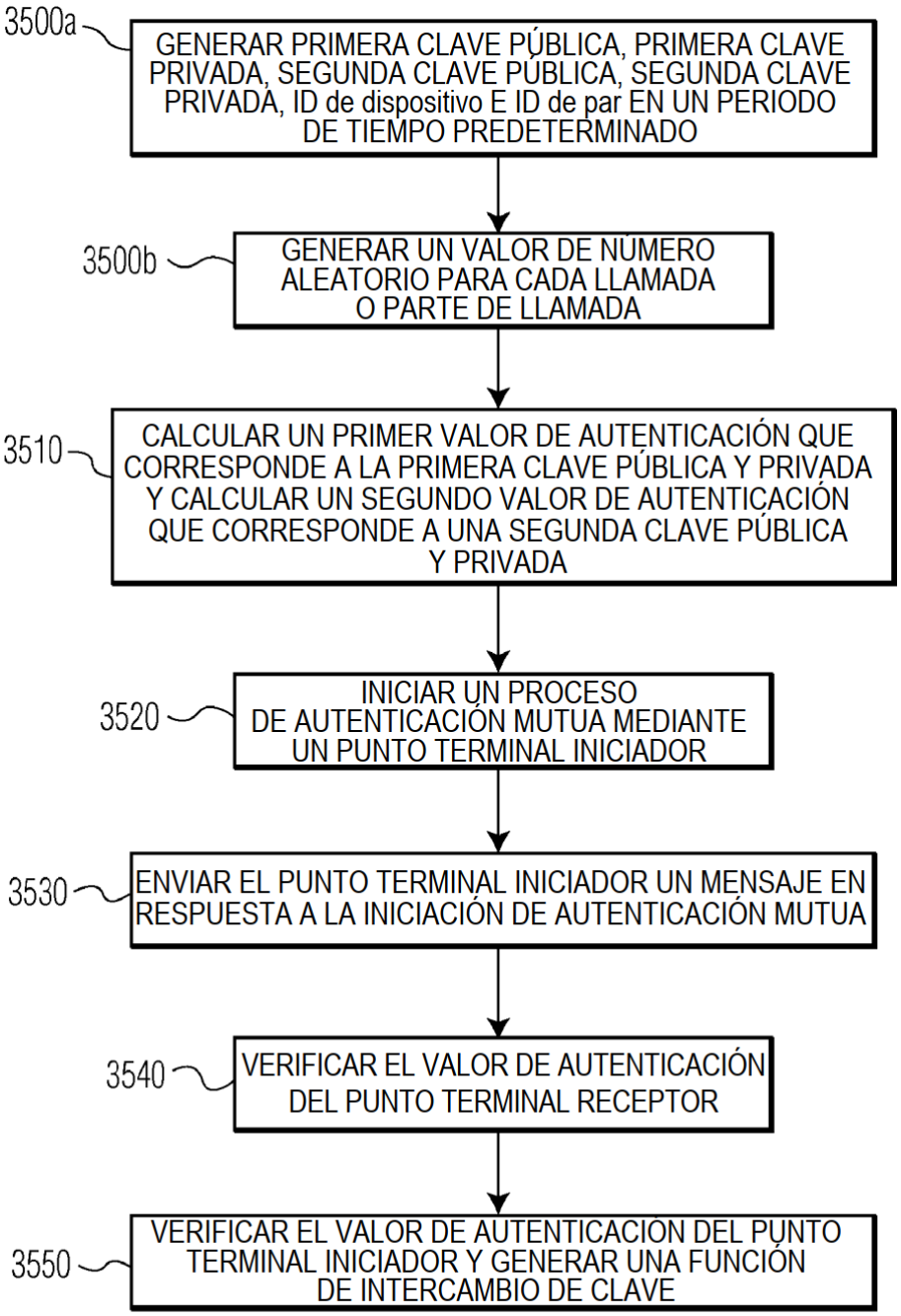
3500a
GENERAR PRIMERA CLAVE PÚBLICA, PRIMERA CLAVE PRIVADA, SEGUNDA CLAVE PÚBLICA, SEGUNDA CLAVE PRIVADA, ID de dispositivo E ID de par EN UN PERIODO DE TIEMPO PREDETERMINADO
3500b
GENERAR UN VALOR DE NÚMERO ALEATORIO PARA CADA LLAMADA O PARTE DE LLAMADA
3510
CALCULAR UN PRIMER VALOR DE AUTENTICACIÓN QUE CORRESPONDE A LA PRIMERA CLAVE PÚBLICA Y PRIVADA Y CALCULAR UN SEGUNDO VALOR DE AUTENTICACIÓN QUE CORRESPONDE A UNA SEGUNDA CLAVE PÚBLICA Y PRIVADA
3520
INICIAR UN PROCESO DE AUTENTICACIÓN MUTUA MEDIANTE UN PUNTO TERMINAL INICIADOR
3530
ENVIAR EL PUNTO TERMINAL INICIADOR UN MENSAJE EN RESPUESTA A LA INICIACIÓN DE AUTENTICACIÓN MUTUA
3540
VERIFICAR EL VALOR DE AUTENTICACIÓN DEL PUNTO TERMINAL RECEPTOR
3550
VERIFICAR EL VALOR DE AUTENTICACIÓN DEL PUNTO TERMINAL INICIADOR Y GENERAR UNA FUNCIÓN DE INTERCAMBIO DE CLAVE

FIG. 3A

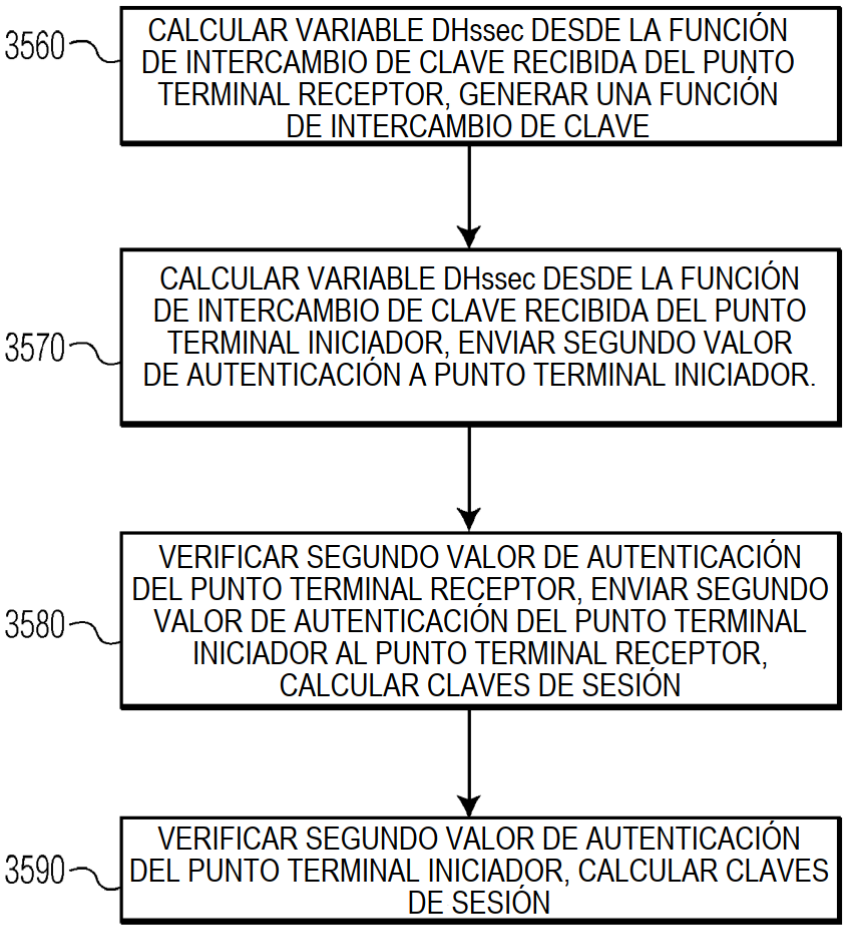
3560
CALCULAR VARIABLE DHssec DESDE LA FUNCIÓN DE INTERCAMBIO DE CLAVE RECIBIDA DEL PUNTO TERMINAL RECEPTOR, GENERAR UNA FUNCIÓN DE INTERCAMBIO DE CLAVE
3570
CALCULAR VARIABLE DHssec DESDE LA FUNCIÓN DE INTERCAMBIO DE CLAVE RECIBIDA DEL PUNTO TERMINAL INICIADOR, ENVIAR SEGUNDO VALOR DE AUTENTICACIÓN A PUNTO TERMINAL INICIADOR.
3580
VERIFICAR SEGUNDO VALOR DE AUTENTICACIÓN DEL PUNTO TERMINAL RECEPTOR, ENVIAR SEGUNDO VALOR DE AUTENTICACIÓN DEL PUNTO TERMINAL INICIADOR AL PUNTO TERMINAL RECEPTOR, CALCULAR CLAVES DE SESIÓN
3590
VERIFICAR SEGUNDO VALOR DE AUTENTICACIÓN DEL PUNTO TERMINAL INICIADOR, CALCULAR CLAVES DE SESIÓN

FIG. 3B

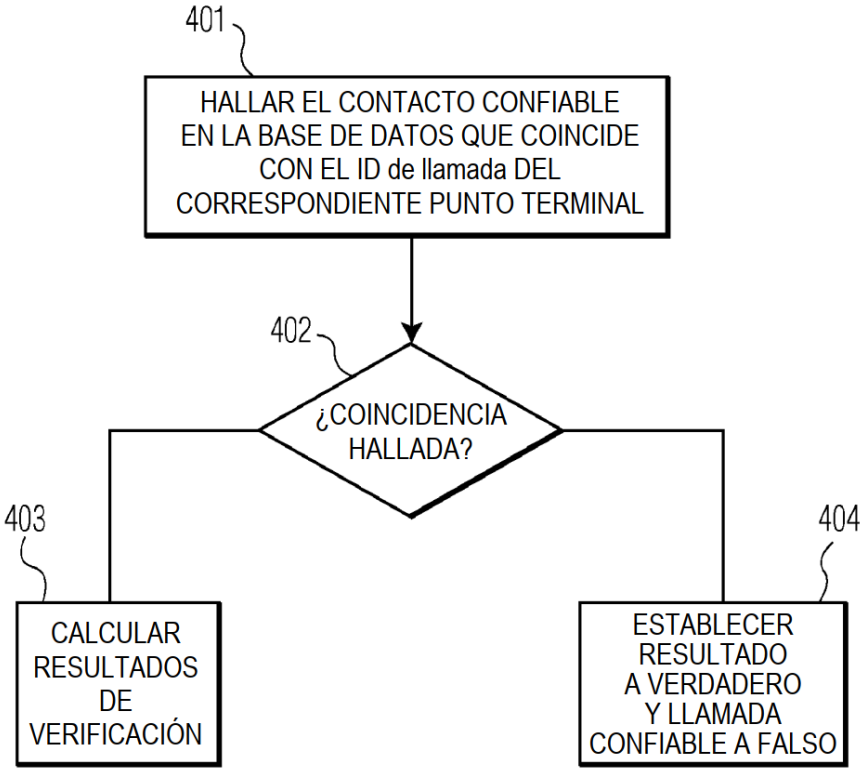
401
HALLAR EL CONTACTO CONFIABLE EN LA BASE DE DATOS QUE COINCIDE CON EL ID de llamada DEL CORRESPONDIENTE PUNTO TERMINAL
402
¿COINCIDENCIA HALLADA?
403
CALCULAR RESULTADOS DE VERIFICACIÓN
404
ESTABLECER RESULTADO A VERDADERO Y LLAMADA CONFIABLE A FALSO

FIG. 4

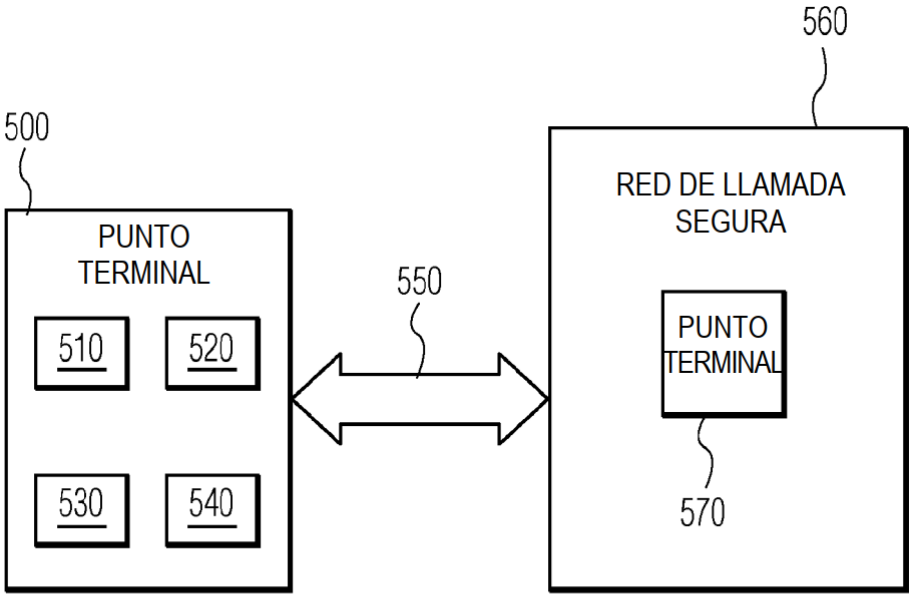
560
500
RED DE LLAMADA SEGURA
PUNTO TERMINAL
550
510
520
PUNTO TERMINAL
530
540
570

FIG. 5