(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 667 104**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04N 7/16 (2011.01)
H04W 4/20 (2008.01)
H04N 21/80 (2011.01)
H04W 4/14 (2009.01)
H04W 4/18 (2009.01)
H04W 88/06 (2009.01)
H04W 84/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **11.03.2015 PCT/EP2015/055076**

(87) Fecha y número de publicación internacional: **17.09.2015 WO15135991**

(96) Fecha de presentación y número de la solicitud europea: **11.03.2015 E 15709669 (4)**

(97) Fecha y número de publicación de la concesión europea: **24.01.2018 EP 3117579**

(54) Título: **Un método y sistema para crear un canal de comunicación seguro entre dos módulos de seguridad**

(30) Prioridad:

11.03.2014 US 201414205209

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.05.2018

(73) Titular/es:

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

(72) Inventor/es:

MELIA, TELEMACO y
SARDA, PIERRE

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Un método y sistema para crear un canal de comunicación seguro entre dos módulos de seguridad

Antecedentes

Este documento se refiere a comunicación electrónica segura y controlar el acceso físico a una red de comunicación.

Los usuarios de servicios de satélite reciben contenido multimedia a través de un enlace descendente de satélite. Algunas redes de satélite convencionales son unidireccionales puesto que no existe una manera para que los usuarios comuniquen de vuelta mediante una red de comunicación bidireccional a la red de satélites. Los recientes avances en tecnologías inalámbricas, por ejemplo, tecnologías inalámbricas celulares de 3G y 4G, han hecho posible proporcionar un canal de comunicación inalámbrica mediante el cual los usuarios de televisión por satélite pueden comunicar con la red de satélites.

Sumario

El presente documento desvela técnicas para emparejamiento seguro de dos módulos de seguridad diferentes (por ejemplo, una tarjeta inteligente) que son operables en dos redes diferentes para un uso emparejado. En algunas implementaciones, una tarjeta inteligente, por ejemplo, como se usa en redes de cable digital o de televisión por satélite, y una tarjeta de Módulo de Identidad de Abonado (SIM), por ejemplo, como se usa en la red de telefonía celular, se despliegan en una instalación de usuario y se emparejan de manera segura juntas de modo que la tarjeta SIM puede usarse para comunicación inalámbrica únicamente siempre que permanezca emparejada con la tarjeta inteligente.

En un aspecto, se proporciona un método para controlar la operación de un primer módulo de seguridad operable en una primera red de comunicación por un segundo módulo de seguridad operable en una segunda red de comunicación. El método incluye enviar un mensaje de inicialización desde la primera red de comunicación a la segunda red de comunicación, identificando de manera inequívoca el mensaje de inicialización el primer módulo de seguridad, generar un secreto basándose en el mensaje de inicialización, comunicar el secreto al primer módulo de seguridad mediante la primera red de comunicación, transmitir el secreto al segundo módulo de seguridad mediante la segunda red de comunicación; y establecer, usando el secreto, un canal seguro entre el segundo módulo de seguridad y el primer módulo de seguridad mediante un tercer enlace de comunicación que es diferente de la primera red de comunicación y la segunda red de comunicación.

En otro aspecto, se desvela un aparato para operación en un sistema de comunicación. El aparato incluye un módulo que envía un mensaje de inicialización a un servidor de aplicaciones mediante una red de comunicación inalámbrica, un módulo que recibe un secreto que se generó basándose en una identidad incluida en el mensaje de inicialización, un módulo que establece un canal de comunicación seguro a través de un enlace de comunicación de área doméstica, y un módulo que envía un mensaje de acuse de recibo mediante la red de comunicación inalámbrica, que indica establecimiento satisfactorio del canal de comunicación seguro.

Estos, y otros aspectos, se describen a continuación en los dibujos, la descripción y las reivindicaciones.

Breve descripción de los dibujos

La Figura 1 ilustra un ejemplo de un sistema de comunicación.

La Figura 2 es un diagrama de bloques representación de un ejemplo de flujo de datos en una red de comunicación.

Descripción detallada

Con los recientes avances en tecnologías de comunicación digital, algunas redes de comunicación tradicionales se están complementando ahora por maneras adicionales para proporcionar datos a usuarios y recibir datos desde usuarios. En muchas localizaciones, por ejemplo, los hogares o empresas de los usuarios o lugares públicos tales como tiendas y aeropuertos, un usuario puede tener múltiples posibilidades para conectar a una red tal como Internet. Por ejemplo, en un hogar del usuario, un usuario puede recibir programas de audio/vídeo y datos mediante una red de satélites o una de cable. Al mismo tiempo, un usuario puede recibir programas de audio/vídeo y datos mediante una red celular inalámbrica tal como una red de 3G o de 4G. De manera similar, en un aeropuerto, un usuario puede establecer conectividad de datos usando su red de datos celular y/o usando un punto caliente inalámbrico o una red Wi-Fi.

Como otro ejemplo, algunos proveedores de programación de televisión por satélite pueden desear complementar su red de comunicación por satélite con una red celular para proporcionar una manera adicional para proporcionar conectividad de datos/contenido en las instalaciones del usuario. Haciendo disponible tal conectividad de dos redes

puede beneficiar tanto a los usuarios como a los proveedores de servicio de red proporcionando oportunidades para proporcionar contenido adicional y servicios, un canal inverso en el que los usuarios pueden comunicar con la red, y la posibilidad de factura mensual reducida para un usuario consolidando los servicios de comunicación, entre otros. Como consecuencia, puede enviarse un contenido multimedia a través de la red de satélites unidireccional a un receptor y un contenido de valor añadido, relacionado con el contenido multimedia puede enviarse a través de la red celular. Mientras se disfruta de un contenido multimedia, el usuario puede activar función mejorada tal como un hiperenlace en los metadatos del contenido multimedia. El hiperenlace se pasará a través del canal seguro al receptor celular (Encaminador de LTE por ejemplo) y a continuación se encaminará al extremo de cabecera de CAS mediante la entidad de gestión móvil. El extremo de cabecera de CAD puede preparar un contenido de valor añadido y transmitirlo mediante la red celular hasta el STB.

La Figura 1 ilustra un ejemplo de un sistema de comunicación. Un sistema de difusión (CAS HD) puede proporcionar contenido mediante un enlace de satélite SNET a una instalación del usuario DEV2. La señal de satélite desde el satélite SNET puede recibirse mediante una antena de tejado, por ejemplo, una antena parabólica. La instalación del usuario puede estar equipada con un decodificador de salón o un receptor DEV2 para recibir el contenido de satélite llevado en la señal de satélite recibida. El receptor DEV2 puede incluir un sistema de desencriptación que usa una tarjeta inteligente SC para proporcionar acceso condicional a diversos programas de televisión que se transmiten a través del enlace satélite SNET. Se ha de observar que el primer módulo de seguridad S1 y el segundo módulo de seguridad S2 incluyen claves de desencriptación para desencriptar datos usando diferentes tecnologías de desencriptación. Adicionalmente, el primer módulo de seguridad y el segundo módulo de seguridad proporcionan diferentes factores de forma físicos y de seguridad.

La instalación del usuario puede también equiparse con un segundo sistema de antenas basándose en un segundo enlace de comunicación inalámbrica FNET diferente del enlace satélite SNET. El segundo sistema de antenas DEV1 puede incluir, por ejemplo, transmisión/recepción de la Evolución a Largo Plazo (LTE) y capacidad de encaminador para proporcionar conexión a Internet por comunicación con una red de LTE FENT. La red de LTE FNET puede incluir una estación base, denominada Nodo B mejorado (eNB), que controla la comunicación inalámbrica en una macro célula. El eNB puede comunicar con la infraestructura de red tal como el núcleo de paquetes evolucionado EPC para proporcionar conectividad a la Internet y otros servicios de telefonía. El contenido de satélite que se transporta a través de la red de satélites FNET, que forma la red troncal para un proveedor de servicio de satélite, puede estar también disponible para el EPC (por ejemplo, para satisfacer interactividad bidireccional por el usuario).

El encaminador de LTE o dispositivo Devl puede estar equipado con un módulo de seguridad (S1) tal como la Tarjeta de Circuito Integrado Universal (UICC), que puede aprovisionarse por el operador móvil (o por el proveedor de UICC). Para el resto de la descripción, el módulo de seguridad se identificará por el SIM, UICC o S1 y hará referencia al módulo de seguridad localizado en el primer dispositivo DEV1. El UICC puede proporcionar parámetros y credenciales, por ejemplo, la Identidad de Abonado Móvil Internacional (IMSI) y la clave de autenticación (Ki), usada para identificar y autenticar al abonado de la red celular. El encaminador de LTE (o DEVI), como cualquier otro dispositivo móvil, está conectado a una MME (Entidad de Gestión Móvil). La MME identifica y autentica el módulo de seguridad (S1) del encaminador de LTE. El encaminador de LTE está localizado adicionalmente mediante la antena móvil más cercana.

Puesto que el encaminador de LTE puede ser una unidad de exteriores, con el UICC también localizado en el exterior de la casa de un usuario, evitar ataques maliciosos puede ser difícil (por ejemplo durante el tiempo nocturno). El clonado del UICC (o de los parámetros contenidos en el UICC) podría dar como resultado uso fraudulento del sistema o incluso que el UICC se venda en el mercado negro. Esto tendría un impacto negativo directo en el servicio proporcionado por el operador de red para el usuario.

El presente documento proporciona, *entre otras cosas,* técnicas para emparejamiento seguro del UICC, también denominada tarjeta de LTE USIM (módulo de identidad de abonado universal) con el módulo de tarjeta inteligente/entorno asegurado en el decodificador de salón de satélite conectado a un canal de difusión. La presente invención se refiere a un método y un sistema como se define en las reivindicaciones.

En algunas realizaciones, el enlace de satélite de canal existente y altamente asegurado SEC_CH se usa para establecer un emparejamiento asegurado entre el UICC y la tarjeta inteligente (S2). Tal emparejamiento, en un aspecto, evita el robo de servicio por un atacante malicioso copiando o robando el UICC y usándolo para otros fines, por ejemplo insertándolo en un teléfono inteligente apto para 4G. En otro aspecto, el emparejamiento puede evitar también que un usuario enchufe el UICC en su teléfono móvil personal para conseguir conexión inalámbrica de 4G mientras se está moviendo, si no está permitido hacer esto por el proveedor de servicio de red. Por ejemplo, en despliegues donde se usa el sistema de antenas 112 en una red de acceso inalámbrico fijo, los eNB pueden configurarse con parámetros para cumplir un cierto requisito de capacidad bajo la suposición de que la tarjeta de UICC no es móvil. En tales sistemas, un movimiento no autorizado del usuario en el UICC puede conducir a configuraciones incorrectas y degradación en la calidad de servicio.

En algunas realizaciones, una comunicación segura (SEC_CH) entre 2 elementos (en este punto la tarjeta SIM y SC), puede establecerse usando un secreto compartido entre ambos elementos. En algunas realizaciones, un

secreto puede crearse en la primera unidad de gestión MME (por ejemplo, infraestructura de red de satélites). Este secreto se comparte a continuación entre la red de satélites y la red celular usando un proceso tal como se describe en este documento. Este secreto se usa a continuación para crear un canal seguro SEC_CH entre el encaminador de LTE (DEV1) y el decodificador de salón (DEV2). El secreto puede usarse como una clave para encriptar los datos intercambiados entre el encaminador de LTE y el decodificador de salón o puede estar en una base en un protocolo Diffie Helmann tal como:

El protocolo Diffie-Hellman es un método para que dos usuarios de ordenador generen una clave privada compartida con la que pueden intercambiar información a través de un canal inseguro. Sean los usuarios con nombres Alice y Bob. En primer lugar, acuerdan dos números primos g y p, donde p es grande (típicamente al menos 512 bits) y g es un módulo de raíz primitiva p. (En la práctica, es una buena idea elegir p de manera que (p-1)/2 también sea primo). Uno de p o g puede generarse a partir del valor secreto. Los números g y p no necesitan mantenerse secretos de otros usuarios. Ahora Alice elige un número aleatorio grande como su clave privada y Bob de manera similar elige un número grande b. Alice a continuación calcula A=g^a (mod p), que ella envía a Bob, y Bob calcula B=g^b (mod p), que él envía a Alice.

Ahora tanto Alice como Bob calculan su clave compartida K=g^(ab) (mod p), que Alice calcula como K=B^a (mod p)=(g^b)^a (mod p)
y Bob calcula como K=A^b (mod p)=(g^a)^b (mod p).

Alice y Bob ahora pueden usar su clave compartida K para intercambiar información sin preocuparse por que otros usuarios obtengan esta información. Para que un fisgón potencial (Eve) haga esto, ella necesitaría en primer lugar obtener K=g^(ab) (mod p) conociendo únicamente g, p, A=g^a (mod p) y B=g^b (mod p).

Esto puede hacerse calculando a a partir de A=g^a (mod p) y b a partir de B=g^b (mod p). Este es el problema logarítmico discreto, que es computacionalmente no factible para p grande. Calcular el logaritmo discreto de un número módulo p lleva aproximadamente la misma cantidad de tiempo que factorizar el producto de dos primos del mismo tamaño que p, que es en lo que se basa la seguridad del sistema criptográfico RSA. Por lo tanto, el protocolo Diffie-Hellman es aproximadamente tan seguro como RSA.

La Figura 1 es una representación de diagrama de bloques de un ejemplo de una red de comunicación establecida para emparejamiento. El receptor de salón de satélite (STB) DEV2 y la unidad de antena de exteriores DEV1 pueden estar comunicativamente acoplados entre sí mediante una red local doméstica (H_S) que forma la tercera red de comunicación TNET (por ejemplo, una red Wi-Fi o una red de Ethernet alámbrica). Un conmutador de Ethernet (por ejemplo, un punto de acceso) puede usarse opcionalmente para facilitar el tráfico de red doméstica. Pueden establecerse dos canales de comunicación lógica usando el tercer canal de comunicación (TNET) entre el STB DEV2 y la unidad DEV1 - un canal lógico seguro SEC_CH y un segundo canal HOME_NT, por ejemplo, un canal de comunicación de Ethernet. El canal seguro SEC_CH puede usar comunicación segura que se asegura usando el SC (o S2) y SIM (o S1). La tarjeta SIM (o USIM, S1) se identifica por la MME mientras que el dispositivo móvil que tiene la tarjeta SIM está conectado a la red móvil. La MME está conectada con un servidor de abonado doméstico (HSS) que proporciona credenciales a un servidor de aplicaciones conectado con la segunda unidad de gestión (extremo de cabecera de CAS). El STB (DEV2) puede recibir programación de satélite (es decir canal de difusión) y los credenciales para la unidad SC a través del enlace satélite SNET. Una vez que se consigue el emparejamiento, puede recibirse contenido añadido (por ejemplo, anuncios, datos interactivos, guía de programas, etc.) a través de la conexión celular FNET y proporcionarse al STB DEV2 para mejorar la experiencia de usuario de contenido que visualiza mediante el canal seguro SEC_CH. El Servidor de Aplicación Interactivo (IAS), conectado al extremo de cabecera de CAS puede a continuación comunicar contenido de valor añadido al STB a través de la primera red de comunicación.

Con referencia a la Figura 2, se describen los mensajes de ejemplo intercambiados a través de una primera red FNET, por ejemplo, una red de 4G 302, y una segunda red SNET, por ejemplo, una red de satélites 304, para emparejar los respectivos módulos de encriptación entre sí.

Una inicialización de la conectividad (por ejemplo, durante la instalación en el tejado por un instalador) de la red de 4G (FNET), la tarjeta SIM (es decir, UICC) instalada en un encaminador de LTE usa una miniaplicación preinstalada para comunicar a la MME, usando por ejemplo comunicación (Figura 2, etapa 100) de SMS (sistema de mensajería sencilla). La tarjeta SIM del primer dispositivo DEV1 genera y envía un primer mensaje (INIT_MESS) a la MME mediante la primera red (FNET). La tarjeta SIM se identifica por la red de 4G (para poder comunicar) y en el nivel de la MME a través del número de teléfono, y/u otra información disponible que identifica de manera inequívoca la tarjeta SIM. Esto puede conseguirse a través de un número de identificación contenido en el mensaje de UICC, o la identificación puede hacerse por la OTA de CAS a través de los datos de personal que acompañan el mensaje tal como el número de teléfono. Un mensaje sencillo tal como "INIT" enviado por la tarjeta SIM se identifica a continuación dentro de la red de 4G puesto que el sistema de origen (tarjeta SIM) añade automáticamente datos personales tales como IMSI que permite que la MME identifique de manera inequívoca la tarjeta SIM.

La MME a continuación genera un secreto único que puede ser un valor numérico o alfanumérico. La MME puede usar un generador de secretos que podría ser un generador de número aleatorio.

El secreto único se envía al primer dispositivo DEV1 para la tarjeta SIM a través de la red de 4G (FNET) usando un canal de comunicación seguro de modo que el secreto no se envía en transparente al SIM (por ejemplo, un comando de administrador a través de SMS) (Figura 2, etapa 2).

El secreto se almacena en la tarjeta SIM del primer dispositivo (FDEV).

Un acuse de recibo (por ejemplo, mediante el SMS) puede enviarse opcionalmente en devolución a que la MME confirme la recepción correcta del secreto.

Después de que la MME ha creado el secreto para el SIM, puede transmitir el secreto al extremo de cabecera de CAS (usando la cuenta CAS asociada). Véase la Figura 2, etapa 3.

La MME y el extremo de cabecera de CAS pueden tener diferente sistema de identificación para sus abonados. La MME puede identificar de manera inequívoca el abonado con un identificador único (UI-CO) y el extremo de cabecera de CAS puede identificar de manera inequívoca el abonado con un identificador único (UI-CH). Para determinar el UI CH, la MME puede enviar un mensaje que contiene el secreto y datos de identificación del usuario tal como IMSI o número de teléfono. El extremo de cabecera de CAS puede a continuación buscar en su base de datos la correspondiente identificación única (UI-CH) del usuario que tiene estos datos de configuración.

De acuerdo con una realización de la invención, la MME puede añadir adicionalmente información acerca del dispositivo DEV1 que solicita el emparejamiento. Esta información puede ser el tipo de dispositivo (dispositivo portátil o dispositivo independiente) y esta información puede usarse por el extremo de cabecera de CAD para filtrar la solicitud. Un emparejamiento puede aceptarse únicamente con un dispositivo independiente tal como el encaminador de LTE y definirse si la tarjeta SIM se enchufa en un dispositivo móvil.

De acuerdo con una realización, el encaminador de LTE (o DEV1), antes del proceso de inicialización, puede consultar al decodificador de salón para obtener su identificador único (UI-CH). Esto puede hacerse a través del canal de comunicación (no seguro en ese momento) que enlaza el encaminador de LTE con el decodificador de salón. A continuación, en el mensaje de UICC que inicia el emparejamiento, el UI-CH se añade de modo que la MME, mientras recibe el mensaje de UICC puede extraer el UI-CH. Este UI-CH se usa cuando la MME está enviando el secreto al extremo de cabecera de CAT y el UI-CH se añade al mensaje, permitiendo que el extremo de cabecera de CAS identifique su abonado. La MME puede transmitir información adicional tal como el nombre del abonado de MME para comprobar si el abonado identificado (identificado con el UI-CH) está autorizado al emparejamiento solicitado.

El secreto compartido puede transmitirse desde el extremo de cabecera de CAS al STB identificado, a través del uso del mensaje de gestión de titularidad especializado (EMM), que puede ser específico por usuario (usando la clave del usuario Ku (Figura 2, etapa 4)). Este sistema posibilita transmisión y recepción asegurada de conjuntos de datos para un STB. La transmisión asegurada del conjunto de datos se asegura a través de la encriptación y firma gestionadas por el extremo de cabecera de CAS. Una vez recibido el secreto compartido se gestiona por los elementos asegurados en el STB (SC o Entorno Confiable (NOCS, NASC, NVSR...)), y se almacena de manera segura en el dispositivo para uso adicional.

Después de que el secreto compartido está disponible en ambos lados (SIM y SC), puede generarse instancias de un protocolo de comunicación especializado y asegurado entre ambos elementos (Figura 2, etapa 5), para permitir la transmisión del conjunto de datos desde el STB a la tarjeta SIM (véase SEC CH en la Figura 1). Para conseguir esto, la tarjeta SIM puede tener una miniaplicación especializada lista en ella, para gestionar el protocolo de comunicación especializado con el STB.

Puede enviarse un acuse de recibo final a la MME, para finalizar y validar la transmisión correcta del secreto compartido.

Con el secreto compartido, tiene lugar a continuación un fuerte emparejamiento entre ambos módulos de seguridad en las dos redes diferentes.

Usando el mismo sistema de comunicación (centralizado en la MME), el secreto compartido puede actualizarse regularmente (en ambos lados).

También, a partir del secreto compartido inicial (generado en la MME), pueden generarse secretos secundarios localmente (SIM y SC) para crear claves de sesión, usables para un periodo de tiempo corto, durante las comunicaciones entre SIM y SC.

Ya que la unidad de LTE de 4G puede instalarse en exteriores, podría ser posible obtener acceso al dispositivo, espiar el cable de Ethernet o sustituir el USIM por uno clonado. En algunas realizaciones, puede implementarse una aplicación/miniaplicación en el UICC, que gestiona la conexión segura con el SC de acuerdo con un protocolo seguro. El UICC puede ejecutar múltiples aplicaciones en paralelo, una es el USIM para acceso de red, pueden definirse otras personalizadas de acuerdo con las interfaces convencionales de UICC.

Algunos aspectos beneficiosos de emparejamiento incluyen:

- Crear un enlace fuerte/seguro entre el mundo CAS (SC-STB) y 4G (tarjeta SIM)

- Posibilitar un túnel encriptado en la comunicación entre el SIM y SC/STB.

- Gestionar la protección de datos entre la red de 4G - principalmente datos del operador de CAS, como contenido de vídeo mejorado - al STB. Los datos en la red de 4G transitarán encriptados (realizado intrínsecamente por los protocolos de comunicaciones de la red de 4G) y se desencriptan en el módem de 4G. Por lo tanto, sin un sistema especializado, estos datos se transmitirán transparentes en la red doméstica.

En algunas realizaciones, los datos/contenido ya están encriptados para el usuario final especializado (usuario final de CAS se identifica en la red de 4G a través del enlace de MME-HSS (enlace de extremo de cabecera), o a través del emparejamiento de red doméstica, puede enviarse información especializada al operador de 4G que identifica el usuario de red de CAS y 4G). Por lo tanto los datos pueden encriptarse directamente para el entorno de CAS antes de que se envíen al usuario.

En algunas realizaciones, se encriptan datos por la red de 4G, y se desencriptan en el módem de encaminador de LTE, donde se establece una VPN asegurada desde el módem al STB, usando el emparejamiento. Por lo tanto no se intercambian datos transparentes entre el módem de LTE y el STB. Otros datos de red local pueden permanecer transparentes (por ejemplo, datos de web solicitados por una sesión de http de portátil local, en la red doméstica)

Una ventaja del emparejamiento es que si alguien está intercambiando las tarjetas SIM ya sea de manera intencionada o accidental o se está ejecutando cualquier otro tipo de ataque puede detectarse y el contenido a través del acceso de LTE de 4G no se entregue al decodificador de salón.

También, un aspecto de la técnica es evitar el uso de la tarjeta de SIM de 4G en un entorno diferente que el 4G + CAS, según se ha creado por el emparejamiento.

En caso de que se detecten ataques o modificaciones el decodificador de salón puede enviar un mensaje de bloqueo para detener la entrega de contenido a través de la tecnología de red comprometida (en este caso el acceso celular).

En algunas realizaciones, la validez del emparejamiento puede comprobarse en una base regular. En un aspecto beneficioso, esta comprobación puede verificar y validar a la red de 4G que la tarjeta SIM se usa correctamente según se supone (por ejemplo, en el módem de tejado). De hecho, tal tarjeta SIM puede usarse directamente en un teléfono activado para 4G, y eliminarla del módem de tejado puede ser posible. Usando comprobaciones regulares de la comunicación protegida iniciada por el STB/SC, el sistema de CAS en el hogar puede validar que la tarjeta apropiada está en su lugar y en buen uso. Esta comprobación puede ser regular, o sobre comando, desde el extremo de cabecera de CAS, y puede dar como resultado realimentación de estado inmediato de vuelta al extremo de cabecera, a través de la red de 4G. Si algo falla (por ejemplo, la tarjeta SIM no está presente), a continuación la realimentación puede almacenarse en el STB para carga futura (una vez que la red vuelve a estar en línea). Tal monitorización regular o remota ayuda a tener una imagen clara de la red global, de una manera controlada por CAS. El mal uso de la tarjeta de SIM de 4G podría a continuación identificarse rápidamente, no únicamente en el nivel de la red de 4G, sino también en el nivel de CAS.

La Figura 2 es una representación de diagrama de flujo de un proceso de emparejamiento de un primer módulo de seguridad (la tarjeta SIM) conectado con un primer dispositivo (el encaminador de LTE) operable en la primera red de comunicación (la red de 4G) con un segundo módulo de seguridad (el módulo de SC) conectado con un segundo dispositivo (el STB) operable en una segunda red de comunicación (el canal de difusión), mediante el cual la operación del primer módulo de seguridad está controlado por el segundo módulo de seguridad.

En 100, se envía un mensaje de inicialización desde el primer dispositivo a través de la primera red de comunicación a la MME que solicita una inicialización de la comunicación con el STB, identificando de manera inequívoca el mensaje de inicialización el primer módulo de seguridad.

En la MME, se genera un secreto basándose en el mensaje de inicialización.

En 101, el secreto se envía al primer módulo de seguridad mediante la primera red de comunicación.

En 102, el secreto se envía por la MME al CAD HD, con una identificación del SIM

En 103, el secreto se transmite al segundo dispositivo mediante la segunda red de comunicación y se carga en el segundo módulo de seguridad (S2).

En 104, usando el secreto, se establece un canal seguro entre el segundo módulo de seguridad y el primer módulo de seguridad mediante un tercer enlace de comunicación que es diferente de la primera red de comunicación y la segunda red de comunicación. El tercer enlace de comunicación puede establecerse, por ejemplo, como una red de área doméstica (alámbrica o inalámbrica) tal como una red Wi-Fi o puede ser un enlace de comunicación de tipo entre pares, por ejemplo, usando conectividad de Ethernet alámbrica o de USB usando el modo entre pares de Bluetooth o Wi-Fi.

En algunas realizaciones, el método incluye adicionalmente verificar periódicamente la presencia del primer módulo de seguridad en el tercer enlace de comunicación, o la red de comunicación a través de la que opera el tercer enlace de comunicación, y emitir un mensaje de error cuando la verificación falla. Puede activar la desactivación, tras recibir el mensaje de error, la operación del segundo módulo de seguridad en la segunda red de comunicación. Para ese fin, el mensaje que contiene el secreto enviado por el extremo de cabecera de CAS puede contener adicionalmente la identificación (por ejemplo IMSI) del primer módulo de seguridad. El segundo módulo de seguridad puede a continuación consultar el primer módulo de seguridad para obtener su IMSI actual y a continuación comparar con la recibida mientras se crea el canal seguro.

En algunas realizaciones desveladas, un sistema para proporcionar contenido a través de una primera red de comunicación y una segunda red de comunicación incluye un primer módulo de seguridad (por ejemplo, una tarjeta de SIM) y un segundo módulo de seguridad (por ejemplo, una tarjeta inteligente) operable en una instalación de un usuario, una primera unidad de gestión (por ejemplo, MME) que opera en la primera red de comunicación (por ejemplo, FNET), configurada para enviar un mensaje de inicialización desde la primera red de comunicación a la segunda red de comunicación (por ejemplo, SNET), identificando de manera inequívoca el mensaje de inicialización el primer módulo de seguridad, un generador de secretos (por ejemplo, un servidor de generación de clave de encriptación o una aplicación de software o una combinación de hardware/software) que genera un secreto basándose en el mensaje de inicialización, un servidor de aplicaciones que comunica el secreto al primer módulo de seguridad mediante la primera red de comunicación, y transmite el secreto al segundo módulo de seguridad mediante la segunda red de comunicación, y provoca que el segundo módulo de seguridad establezca, usando el secreto, un canal seguro (por ejemplo, usando un túnel de IP Sec, una conexión de SSL, etc.) entre el segundo módulo de seguridad y el primer módulo de seguridad mediante un tercer enlace de comunicación (una conexión entre pares como se ha descrito anteriormente, o parte de una red de área doméstica) que es diferente de la primera red de comunicación y la segunda red de comunicación.

Se apreciará que se desvelan técnicas para emparejar hasta dos módulos de seguridad diferentes que usan dos tecnologías de encriptación diferentes para operación en dos redes diferentes. En un aspecto ventajoso, uno de los módulos de seguridad, que puede ser propenso para duplicación o robo, se ancla lógicamente al otro módulo de seguridad mediante el emparejamiento. Por ejemplo, después de que se realiza satisfactoriamente el emparejamiento, el primer módulo de seguridad puede usarse en una red de área extensa únicamente cuando su presencia en una red local, tal como una red de un abonado, o una red de comunicación de campo cercano, puede detectarse y verificarse por el segundo módulo de seguridad.

Se apreciará adicionalmente que las técnicas desveladas pueden usarse para proporcionar un canal interactivo bidireccional para llevar a cabo contenido de valor añadido fuera de banda al usuario y llevar mensajes de interacción de usuario para la red a una red unidireccional tradicional tal como una red de televisión de pago por satélite. El Servidor de Aplicación Interactivo (IAS) puede enviar contenido especializado a un único usuario y encaminará el contenido añadido mediante la MME y la primera red de comunicación. El canal interactivo bidireccional puede usar una tecnología ya existente tal como LTE, pero al mismo tiempo, proteger el equipo de piratería o uso no autorizado emparejando de manera segura el receptor celular con la identidad del abonado de TV de pago de satélite.

Las realizaciones desveladas y otras, las operaciones y módulos funcionales descritos en este documento pueden implementarse en circuitería electrónica digital o en software informático, firmware o hardware, que incluye las estructuras desveladas en este documento y sus equivalentes estructurales, o en combinaciones de uno o más de ellos. Las realizaciones desveladas y otras pueden implementarse como uno o más productos de programa informático, es decir, uno o más módulos de instrucciones de programa informático codificadas en un medio legible por ordenador para ejecución por, o para controlar la operación de, el aparato de procesamiento de datos. El medio legible por ordenador puede ser un dispositivo de almacenamiento legible por máquina, un sustrato de almacenamiento legible por máquina, un dispositivo de memoria, una composición de materia que afecta una señal propagada legible por máquina o una combinación de uno o más de ellos. La expresión "aparato de procesamiento de datos" abarca todos los aparatos, dispositivos y máquinas para procesar datos, incluyendo a modo de ejemplo un procesador programable, un ordenador, o múltiples procesadores u ordenadores. El aparato puede incluir, además de hardware, código que crea un entorno de ejecución para el programa informático en cuestión, por ejemplo, código

que constituye el firmware de procesador, una pila de protocolo, un sistema de gestión de base de datos, un sistema operativo, o una combinación de uno o más de ellos. Una señal propagada es una señal generada artificialmente, por ejemplo, una señal eléctrica, óptica o electromagnética generada por máquina, que se genera para codificar información para transmisión al aparato receptor adecuado.

Un programa informático (también conocido como un programa, software, aplicación de software, guion o código) puede escribirse en cualquier forma de lenguaje de programación, incluyendo lenguajes compilados o interpretados, y puede desplegarse en cualquier forma, incluyendo como un programa independiente o como un módulo, componente, subrutina u otra unidad adecuada para uso en un entorno informático. Un programa informático no corresponde necesariamente a un fichero en un sistema de ficheros. Un programa puede almacenarse en una porción de un fichero que mantiene otros programas o datos (por ejemplo, uno o más guiones almacenados en un documento de lenguaje de marcas), en un único fichero especializado al programa en cuestión, o en múltiples ficheros coordinados (por ejemplo, ficheros que almacenan uno o más módulos, subprogramas o porciones de código). Un programa informático puede desplegarse para ejecutarse en un ordenador o en múltiples ordenadores que están localizados en un sitio o distribuidos a través de múltiples sitios e interconectados por una red de comunicación.

Los procesos y flujos lógicos descritos en este documento pueden realizarse por uno o más procesadores programables que ejecutan uno o más programas informáticos para realizar funciones operando en datos de entrada y generando salida. Los procesos y flujos lógicos pueden realizarse también por, y el aparato puede implementarse también como, circuitería de lógica de fin especial, por ejemplo, un FPGA (campo de matriz de puertas programables) o un ASIC (circuito integrado específico de la aplicación).

Los procesadores adecuados para la ejecución de un programa informático incluyen, a modo de ejemplo, tanto microprocesadores de fin general como especial, y cualquiera de uno o más procesadores de cualquier clase de ordenador digital. En general, un procesador recibirá instrucciones y datos desde una memoria de sólo lectura o memoria de acceso aleatorio o ambas. Los elementos esenciales de un ordenador son un procesador para realizar instrucciones y uno o más dispositivos de memoria para almacenar instrucciones y datos. En general, un ordenador incluirá también, o estará operativamente acoplado para recibir datos desde o transferir datos a, o ambas, uno o más dispositivos de almacenamiento masivo para almacenar datos, por ejemplo, magnéticos, discos magneto ópticos, o discos ópticos. Sin embargo, un ordenador no necesita tener tales dispositivos. Medio legible por ordenador adecuado para almacenar instrucciones de programa informático y datos incluye todas las formas de memoria no volátil, medios y dispositivos de memoria, incluyendo a modo de ejemplo dispositivos de memoria de semiconductores, por ejemplo, EPROM, EEPROM, y dispositivos de memoria flash; discos magnéticos, por ejemplo, discos duros internos o discos extraíbles; discos magneto ópticos; y discos de CD ROM y DVD-ROM. El procesador y la memoria pueden complementarse por, o incorporarse en, circuitería de lógica de fin especial.

Aunque este documento contiene muchos detalles específicos, estos no deberían interpretarse como limitaciones en el alcance de una invención que se reivindica o lo que pueda reivindicarse, sino en su lugar como descripciones de características específicas a realizaciones particulares. Ciertas características que se describen en este documento en el contexto de realizaciones separadas pueden implementarse también en combinación en una única realización. A la inversa, diversas características que se describen en el contexto de una única realización pueden implementarse también en múltiples realizaciones de manera separada o en cualquier sub-combinación adecuada. Además, aunque las características pueden haberse descrito anteriormente como actuando en ciertas combinaciones e incluso inicialmente reivindicadas como tal, una o más características de una combinación reivindicada pueden, en algunos casos, suprimirse de la combinación, y la combinación reivindicada puede dirigirse a una sub-combinación o una variación de una sub-combinación. De manera similar, aunque se representan operaciones en los dibujos en un orden particular, esto no debería entenderse como que requiere que tales operaciones se realicen en el orden particular mostrado o en orden secuencial, o que todas las operaciones ilustradas se realicen, para conseguir resultados deseables.

Únicamente se desvelan unos pocos ejemplos e implementaciones. Pueden realizarse variaciones, modificaciones y mejoras a los ejemplos descritos e implementaciones y otras implementaciones basándose en lo que se ha desvelado.

REIVINDICACIONES

1. Un método para crear un canal de comunicación seguro (SEC_CH) entre un primer módulo de seguridad (S1) conectado a un primer dispositivo (DEV1) operable en una primera red de comunicación (FNET) y un segundo módulo de seguridad (S2) conectado a un segundo dispositivo (DEV2) operable en una segunda red de comunicación (SNET), comprendiendo el método:

enviar un mensaje de inicialización (INIT_MESS) desde el primer dispositivo (DEV1) a través de la primera red de comunicación (FNET) a una primera unidad de gestión (MME), identificando de manera inequívoca el mensaje de inicialización el primer módulo de seguridad (S1);
generar por la primera unidad de gestión (MME) un secreto basándose en el mensaje de inicialización; transmitir el secreto al primer módulo de seguridad (S1) mediante la primera red de comunicación (FNET);
transmitir el secreto a una segunda unidad de gestión (CAS HD) conectada a la segunda red de comunicación (SNET);
transmitir el secreto al segundo dispositivo (S2) mediante la segunda red de comunicación (SNET), cargando el secreto en el segundo módulo de seguridad (S2), y
establecer, usando el secreto, el canal seguro (SEC_CH) entre el segundo módulo de seguridad (S2) y el primer módulo de seguridad (S1) mediante un tercer enlace de comunicación (TNET) que es diferente de la primera red de comunicación (FNET) y la segunda red de comunicación (SNET), estando emparejado el primer módulo de seguridad (S1) con el segundo módulo de seguridad (S2) compartiendo el secreto.

2. El método de la reivindicación 1, que comprende adicionalmente:

verificar periódicamente la presencia del primer módulo de seguridad en la tercera red de comunicación por el segundo dispositivo; y
emitir un mensaje de error cuando la verificación falla.

3. El método de la reivindicación 1 o 2, en el que la segunda red de comunicación es una red de comunicación unidireccional.

4. El método de cualquiera de las reivindicaciones 1 a 3, en el que la primera red de comunicación comprende una red celular y en el que el primer módulo de seguridad comprende un módulo de identidad de abonado (SIM).

5. El método de cualquiera de las reivindicaciones 1 a 4, en el que la segunda red de comunicación comprende una red de difusión de satélite.

6. El método de cualquiera de las reivindicaciones 1 a 4, en el que el secreto se transmite a la segunda unidad de gestión con identificación del primer módulo de seguridad; realizando dicho segundo módulo de gestión una búsqueda para determinar la identificación del segundo módulo de seguridad.

7. El método de cualquiera de las reivindicaciones 1 a 6, que comprende adicionalmente:

proporcionar contenido multimedia a través de la segunda red de comunicación; y
proporcionar contenido de valor añadido relacionado con el contenido multimedia a través de la primera red de comunicación.

8. El método de la reivindicación 2, que comprende adicionalmente:

desactivar, tras recibir el mensaje de error, la operación del segundo módulo de seguridad en la segunda red de comunicación.

9. Un sistema para crear un canal seguro entre un primer módulo de seguridad (S1) conectado a un primer dispositivo (DEV1) operable en una primera red de comunicación (FNET) y un segundo módulo de seguridad (S2) conectado a un segundo dispositivo (DEV2) operable en una segunda red de comunicación (SNET), comprendiendo el sistema:

el primer módulo de seguridad (S1) y un segundo módulo de seguridad (S2) operable en una instalación del usuario; una primera unidad de gestión (MME) en la primera red de comunicación, configurada para recibir un mensaje de inicialización mediante la primera red de comunicación desde el primer módulo de seguridad (S1), identificando de manera inequívoca el mensaje de inicialización el primer módulo de seguridad (S1);
un generador de secretos en la primera unidad de gestión (MME) que genera un secreto basándose en el mensaje de inicialización;
estando configurada adicionalmente la primera unidad de gestión (MME) para comunicar el secreto al primer módulo de seguridad mediante la primera red de comunicación; y para transmitir el secreto a una segunda unidad de gestión (CAD HD) conectada a la segunda red de comunicación (SNET);

estando configurada la segunda unidad de gestión (CAD HD) para enviar el secreto al segundo módulo de seguridad (S2) mediante la segunda red de comunicación (SNET); y
provocar que el segundo módulo de seguridad (S2) establezca, usando el secreto, un canal seguro entre el segundo módulo de seguridad (S2) y el primer módulo de seguridad (S1) mediante un tercer enlace de comunicación (TNET) que es diferente de la primera red de comunicación (FNET) y la segunda red de comunicación (SNET), estando emparejado el primer módulo de seguridad (S1) con el segundo módulo de seguridad (S2) compartiendo el secreto.

10. El sistema de la reivindicación 9, en el que el segundo módulo de seguridad está configurado adicionalmente para:

verificar periódicamente la presencia del primer módulo de seguridad mediante el tercer enlace de comunicación; y emitir un mensaje de error cuando la verificación falla.

11. El sistema de la reivindicación 9 o 10, en el que la segunda red de comunicación es una red de comunicación unidireccional.

12. El sistema de cualquiera de las reivindicaciones 9 a 11, en el que la primera red de comunicación comprende una red celular y en el que el primer módulo de seguridad comprende un módulo de identidad de abonado.

13. El sistema de cualquiera de las reivindicaciones 9 a 12, en el que la segunda red de comunicación comprende una red de difusión de satélite.

14. El sistema de cualquiera de las reivindicaciones 9 a 13, en el que el tercer enlace de comunicación comprende una red de instalaciones del usuario.

15. El sistema de cualquiera de las reivindicaciones 9 a 14, que comprende adicionalmente:

un extremo de cabecera que proporciona contenido multimedia a través de la segunda red de comunicación; y
un servidor de aplicación interactivo que proporciona contenido de valor añadido relacionado con el contenido multimedia a través de la primera red de comunicación.

16. El sistema de la reivindicación 10, en el que la primera red de comunicación comprende un servidor de autenticación que desactiva, tras recibir el mensaje de error, la operación del segundo módulo de seguridad en la segunda red de comunicación.

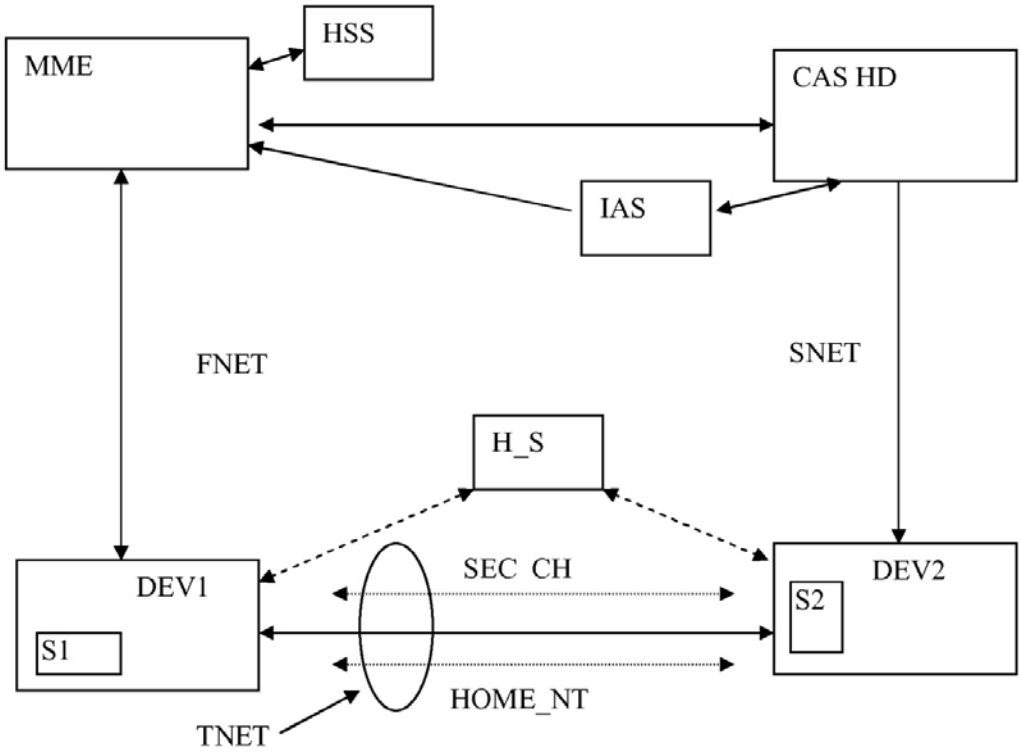
MME
HSS
CAS HD
IAS
FNET
SNET
H_S
DEV1
S1
SEC CH
DEV2
S2
HOME_NT
TNET

FIG. 1

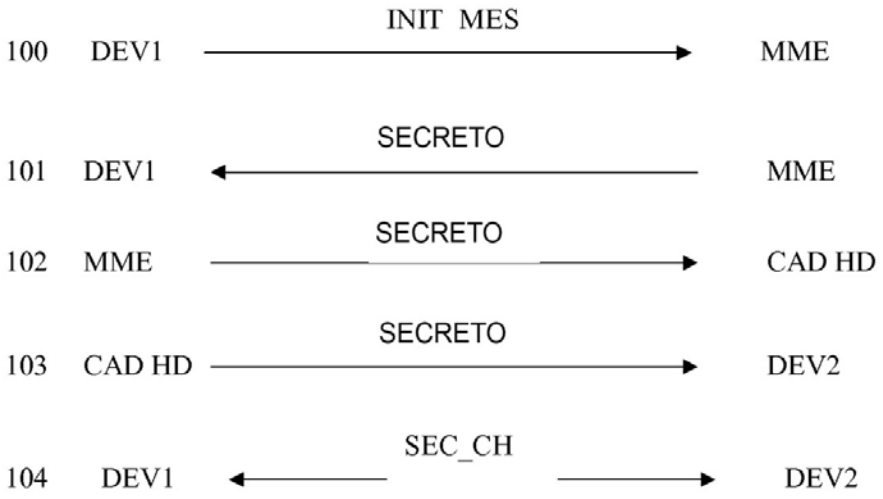
INIT MES
100 DEV1
MME
SECRETO
101 DEV1
MME
SECRETO
102 MME
CAD HD
SECRETO
103 CAD HD
DEV2
SEC_CH
104 DEV1
DEV2

FIG. 2