(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 358 055**

(51) Int. Cl.:
H04L 9/08 (2006.01)
H04L 12/18 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07727160 .9**
(96) Fecha de presentación : **21.03.2007**
(97) Número de publicación de la solicitud: **2014010**
(97) Fecha de publicación de la solicitud: **14.01.2009**

(54) Título: **Procedimiento, dispositivo y producto de programa de computadora para codificar y decodificar datos de medios.**

(30) Prioridad: **21.04.2006 DE 10 2006 018 645**

(45) Fecha de publicación de la mención BOPI:
05.05.2011

(45) Fecha de la publicación del folleto de la patente:
05.05.2011

(73) Titular/es:
NOKIA SIEMENS NETWORKS GmbH & Co. KG.
St. Martin Strasse 76
81541 München, DE

(72) Inventor/es: **Thiruvengadam, Srinath**

(74) Agente: **Zuazo Araluze, Alexander**

DESCRIPCION

La invención se refiere a un procedimiento para codificar y decodificar datos de medios en un sistema de comunicaciones. La invención se refiere además a un aparato de abonado y a un servidor de control como partes de un sistema de comunicaciones, así como a un producto de programa de computadora, con los que puede realizarse el procedimiento.

Al aumentar la difusión de las redes de telefonía móvil de banda ancha, por ejemplo UMTS (Universal Mobile Telecommunication System, sistema universal móvil de telecomunicaciones), ha desarrollado el llamado proyecto de colaboración de la tercera generación (Third Generation Partnership Project, 3GPP) una serie de estándares para la integración de servicios de voz e Internet bajo el nombre de subsistemas multimedia de IP (IMS). Los estándares IMS deben impulsar la fusión de redes de conmutación por paquetes y de conmutación por línea, en particular en el ámbito móvil. No obstante, los sistemas IMS son también adecuados para transmitir datos de medios en redes fijas, por ejemplo a través de redes telefónicas públicas o de Internet.

En redes de telefonía móvil según el estándar 3GPP red de acceso de radio terrestre de UMTS (UMTS Terrestrial Radio Access Network, UTRAN) se codifican datos sobre uno de los niveles de transmisión inferiores del protocolo de red, por ejemplo en la capa de seguridad. Por ello no prevén los estándares de seguridad de acceso IMS, IMS Access Security (3GPP TS 33.203) y de seguridad de dominio de red, Network Domain Security (3GPP TS 33.210) ninguna codificación separada de datos de medios. No obstante, en redes fijas no se realiza una tal codificación de datos transmitidos.

No obstante, a menudo se desea una codificación de datos de medios, ya que por un lado en particular las redes que se basan en el protocolo de Internet (IP) son notoriamente inseguras, con lo que por ejemplo las conferencias por videoteléfono, que al menos en parte se llevan a cabo a través de tales redes, pueden ser escuchadas indebidamente con relativa facilidad. Por otro lado, se ofrecen datos de medios a menudo como los llamados servicios de valor añadido sujetos a costes, como por ejemplo el video sobre demanda (Video-on-Demand). También aquí debe quedar asegurado que los datos de medios transmitidos sólo son utilizados por el receptor autorizado.

Un estándar para la transmisión segura de datos de medios entre dos abonados se conoce por ejemplo con el protocolo de transporte seguro en tiempo real (Secure Realtime Transport Protocol, SRTP, correspondiente a RFC 3711). Una transmisión de datos según el estándar SRTP no puede no obstante utilizarse en particular en redes heterogéneas, ya que en parte en los límites de la red, por ejemplo en la transición de Internet a redes telefónicas públicas, se producen problemas técnicos en la conversión de flujos de datos codificados.

Es por lo tanto tarea de la invención describir procedimientos y dispositivos de un sistema de comunicaciones en los que sea posible una codificación de datos de medios para la transmisión en una red de medios de manera sencilla y segura.

La tarea se resuelve mediante las características de las reivindicaciones independientes. Ventajosas configuraciones mejoradas de la invención se caracterizan en las correspondientes reivindicaciones dependientes.

Según un primer aspecto, se caracteriza la invención por un procedimiento para codificar y decodificar datos de medios que presenta los siguientes pasos: Se transmite una consulta desde un aparato de abonado a través de una red de control a un servidor de control para determinar un conjunto de parámetros de codificación para datos de control. Entonces incluye la consulta datos de identificación del aparato de abonado. El servidor de control determina a continuación el conjunto de parámetros de codificación para los datos de control, incluyendo un número aleatorio, una clave de datos de control y una clave de integridad, dependiendo la clave de datos de control y la clave de integridad del número aleatorio y de los datos de identificación. A continuación se genera una clave de medios en función de la clave de los datos de control y de la clave de integridad mediante el servidor de control y se transmite a través de una red núcleo a un servidor de medios. A continuación se codifican los datos de medios no codificados mediante el servidor de medios utilizando la clave de medios para su envío a través de una red de datos al aparato de abonado y/o se decodifican los datos de medios codificados recibidos a través de la red de datos y enviados por un aparato de abonado utilizando la clave de medios mediante el servidor de medios.

Para codificar los datos de control en un sistema de comunicaciones es imprescindible acordar la clave de datos de control y dado el caso adicionalmente la clave de integridad entre el aparato de abonado y el servidor de control. Debido a que la clave de medios se determina a partir de estas claves ya conocidas, puede renunciarse a un acuerdo adicional sobre la clave de medios. Ventajosamente se reducen así tanto el tráfico en la red como la potencia de cálculo que serían necesarios por ejemplo para una autentificación del aparato de abonado frente al servidor de control cuando se acordase separadamente la clave de medios.

Según una configuración ventajosa del primer aspecto, se transmiten adicionalmente a la clave de medios otros parámetros de codificación, en particular relativos al algoritmo de codificación a utilizar, desde el servidor de control a través de la red núcleo al servidor de medios. De esta manera puede utilizarse el procedimiento universalmente en distintos contextos de codificación.

Ventajosamente fija entonces previamente el aparato de abonado los otros parámetros de codificación, transmitiéndolos al servidor de control, o se acuerdan entre el aparato de abonado y el servidor de control. De esta manera se logra que para ambas partes, aparato de abonado y servidor de control o bien servidor de medios, se utilicen parámetros de codificación adecuados, es decir, por ejemplo un algoritmo de codificación adecuado, conocido por ambas partes.

La tarea se resuelve según un segundo aspecto igualmente mediante un procedimiento en el que, análogamente al primer aspecto, se transmite una consulta desde un aparato de abonado a través de una red de control a un servidor de control para determinar un conjunto de parámetros de codificación para datos de control. Del bloque de parámetros de codificación generado a continuación se envía de retorno un número aleatorio al aparato de abonado. El aparato de abonado genera en base a datos de identificación y al número aleatorio una clave de datos de control y una clave de integridad. A continuación se genera una clave de medios en función de la clave de datos de control y de la clave de integridad mediante el aparato de abonado. A continuación se decodifican los datos de medios codificados recibidos a través de la red de datos, enviados por un servidor de medios, utilizando la clave de medios, mediante el aparato de abonado y/o se codifican los datos de medios no codificados mediante el aparato de abonado utilizando la clave de medios para su envío a través de una red de datos al servidor de medios. Las ventajas que resultan se corresponden con las del primer aspecto.

Según otras configuraciones ventajosas de la invención, se forma la clave de medios bien mediante una combinación O-exclusiva (XOR) o con ayuda de una función Hash de una vía a partir de la clave de datos de control y de la clave de integridad. Ambas son funciones fáciles de implementar y ofrecen el aspecto de seguridad ventajoso de que a partir de la clave de medios no pueden deducirse la clave de datos de control y la clave de integridad. Cuando se utiliza una función Hash de una vía, no puede averiguarse incluso conociendo la clave de medios y una de las otras dos claves la tercera clave.

Según otras configuraciones ventajosas de la invención, se determina la clave de medios bien directamente para la codificación y decodificación o bien se determina en función de la clave de medios otra clave, que se utiliza para la codificación y decodificación.

Según un tercer aspecto, se resuelve la tarea igualmente mediante un servidor de control de un sistema de comunicaciones con una primera interfaz hacia a una red de control y una segunda interfaz hacia una red núcleo. El servidor de control puede unirse entonces a través de la primera interfaz y la red de control con un aparato de abonado y a través de la segunda interfaz y la red núcleo con un servidor de medios. El servidor de control está equipado para recibir datos de identificación del aparato de abonado y determinar un conjunto de parámetros de codificación para datos de control. Los parámetros de codificación incluyen entonces un número aleatorio y, en función del número aleatorio y de los datos de identificación, una clave de datos de control y una clave de integridad. El servidor de control está además equipado para generar una clave de medios en función de la clave de datos de control y de la clave de integridad y transmitirla a través de la red núcleo al servidor de medios.

Análogamente se resuelve la tarea según un cuarto aspecto mediante un aparato de abonado para su utilización en un sistema de comunicaciones con una primera interfaz hacia una red de control y una segunda interfaz hacia una red de medios. El aparato de abonado puede unirse entonces a través de la primera interfaz y de la red de control para el intercambio de datos de control con un servidor de control y mediante la segunda interfaz y la red de medios para el intercambio de datos de medios con un servidor de medios. El aparato de abonado está equipado para enviar datos de identificación al servidor de control, recibir como respuesta un número aleatorio y generar una clave de datos de control y una clave de integridad en función del número aleatorio y los datos de identificación, sirviendo la clave de datos de control y la clave de integridad para codificar y decodificar los datos de control. El aparato de abonado está además equipado para generar una clave de medios en función de la clave de datos de control y de la clave de integridad, sirviendo la clave de medios para codificar y decodificar los datos de medios.

Según un quinto aspecto, se resuelve la tarea mediante un producto de programa de computadora con código de programa para ejecutar un programa de computadora en una o varias computadoras de un sistema de comunicaciones, ejecutándose cuando se ejecuta el código del programa uno de los procedimientos indicados.

Al igual que el producto de programa de computadora, permiten el servidor de control y el aparato de abonado realizar el procedimiento correspondiente a la invención. Las ventajas que resultan del tercer, cuarto y quinto aspecto corresponden por lo tanto a las del primer y segundo aspecto.

La invención se describirá a continuación más en detalle en base a ejemplos de ejecución con ayuda de tres figuras. Las figuras muestran:

figura 1 un sistema de comunicaciones con un aparato de abonado, un servidor de control y un servidor de medios,

figura 2 una configuración de un servidor de control y

figura 3 un diagrama secuencial del establecimiento de un enlace y una transmisión a continuación de datos de medios codificados desde un servidor de medios a un aparato de abonado.

La figura 1 muestra un sistema de comunicaciones, que presenta un aparato de abonado 1 con datos de identificación ID, que está unido mediante una red de control 2 con un servidor de control 3. A través de la red de control 2 pueden transmitirse por ejemplo los datos de identificación ID y un número aleatorio R. El servidor de control 3 presenta parámetros de codificación K que incluyen una clave de datos de control CK, una clave de integridad IK y el número aleatorio R. El servidor de control 3 está unido mediante una red núcleo 4, que transmite una clave de medios MD, con un servidor de medios 5, que presenta datos de medios MD no codificados. El servidor de medios 5 está unido a su vez a través de una red de datos 6 mediante la que se transmiten datos de medios codificados CMD, con el aparato de abonado 1. El servidor de control 3, la red núcleo 4 y el servidor de medios 5 constituyen un puesto de conmutación 7 o son parte del mismo. La red de control 2 y la red de datos 6 forman conjuntamente una red de acceso 8. El aparato de abonado 1 y el servidor de control 3 presentan un generador de claves de medios 9.

La configuración mostrada en la figura 1 es un esquema de un sistema de comunicaciones. Para simplificar sólo se ha representado un aparato de abonado 1. Usualmente existen múltiples aparatos de abonado, conectados mediante respectivas redes de acceso con el puesto de conmutación 7. También pueden estar previstos en una red de comunicaciones varios puestos de conmutación, estando conectado un primer grupo de aparatos de abonado a un primer puesto de conmutación y un segundo grupo de aparatos de abonado a un segundo puesto de conmutación. Los distintos puestos de conmutación están unidos en un caso así típicamente tanto mediante sus servidores de control propios como también a través de sus servidores de medios. También puede pensarse, desde luego, en que varios puestos de conmutación con sus respectivos servidores de control propios se sirvan de un servidor de medios común. La conexión entre distintos puestos de conmutación puede realizarse mediante una red correspondiente a la red núcleo 4. Alternativamente puede ser la red núcleo 4 más extensa y extenderse por varios puestos de conmutación.

Un sistema de comunicaciones del tipo descrito es adecuado para transmitir datos y/o conversaciones telefónicas (codificadas como datos) entre dos aparatos de abonado, es decir, por ejemplo el aparato de abonado 1 mostrado y otro aparato de abonado no mostrado a través del servidor de medios 5 y dado el caso otros servidores de medios. Igualmente es posible que el aparato de abonado 1, sin la participación de otro aparato de abonado, reciba datos del servidor de medios 5 o bien los intercambie con el mismo. Un caso así se presenta por ejemplo cuando se utilizan servicios como video sobre demanda.

La red de acceso 8 es por ejemplo una red telefónica pública ligada a línea, como por ejemplo una red telefónica analógica o una red telefónica digital de servicios integrados (ISDN, Integrated Services Digital Network). Otras redes de acceso pueden ser por ejemplo redes de telefonía móvil inalámbricas, como por ejemplo redes GSM (Global System for Mobile Communication, sistema global para la comunicación móvil) o bien redes UMTS. La red núcleo 4 es por ejemplo una red de datos según el protocolo de Internet que utiliza un ofertante de servicios de comunicaciones en o entre puestos de conmutación para la transmisión de datos.

En la red de acceso 8 se transmiten datos de control a través de la red de control 2 y datos útiles a través de la red de medios 6. Al respecto la red de control 2 y la red de medios 6 pueden ser redes físicas separadas, o también redes lógicas separadas de la misma red física. Sólo existen redes separadas lógicamente por ejemplo cuando se intercambian datos de control y datos útiles a través de distintos niveles de protocolo sobre un único canal de transmisión entre el puesto de conmutación 7 y el aparato de abonado 1. Puede tratarse no obstante también de canales de transmisión separados, como por ejemplo un llamado canal de control ISDN D y un llamado canal de datos ISDN B.

En particular cuando la red de acceso 8 es una red telefónica ligada a línea, no deben intercambiarse datos útiles no codificados entre el aparato de abonado 1 y el servidor de medios 5. Para este fin se conocen por el estado de la técnica las unidades de codificación y decodificación 10 en el aparato de abonado 1 y en el servidor de medios 5. Mediante las unidades de codificación y decodificación 10 pueden codificarse datos útiles, por ejemplo los datos de medios MD, en el servidor de medios 5 y transmitirse entonces como datos de medios codificados CMD al aparato de abonado 1 a través de la red de medios 6.

Mediante la unidad de codificación y decodificación 10 del aparato de abonado 1 pueden decodificarse de nuevo los datos de medios codificados CMD recibidos para utilizarlos. Puesto que típicamente se utiliza un procedimiento de codificación simétrico, deben disponer ambas unidades de codificación y decodificación 10 de la misma clave. En el marco de la invención proporcionan para ese fin

los generadores de claves de medios 9 la clave de medios MK a las unidades de codificación y decodificación 10.

En el caso de una red de radio como red de acceso, no sería necesario codificar los datos útiles para transmitirlos, ya que se utiliza una codificación ya en el plano de seguridad del protocolo de la red. No obstante, puede utilizarse el procedimiento correspondiente a la invención también en una red de acceso que utiliza un protocolo de red que se transmite codificado.

La tarea del servidor de control 3 consiste en iniciar controlar y vigilar el establecimiento del enlace entre el aparato de abonado 1 y el puesto de conmutación 7. En la figura 2 se representa más en detalle la estructura de un servidor de control 3 en un ejemplo de ejecución. El servidor de control 3 incluye varios componentes funcionales, equipados para procesar diversas tareas del servidor de control 3, que son un servidor de contacto 3a, un servidor de sesión 3b y un servidor de abonados 3c. El generador de la clave de medios 9 está previsto dentro del servidor de contacto 3a. Desde el servidor de contacto 3a parten también los enlaces con el aparato de abonado 1 y con el servidor de medios 7.

Usualmente están implementados los tres componentes del servidor de control 3 en software, pudiendo estar realizados los componentes sobre una unidad común de hardware o también sobre unidades separadas de hardware. Las unidades separadas de hardware pueden entonces estar también separadas espacialmente, pudiendo utilizarse una red similarmente a la red núcleo 4 para el intercambio de datos.

La estructura mostrada en la figura 2 de un servidor de contacto 3 es típica de un subsistema multimedia IP según los estándares 3GPP. En un tal sistema se denomina al servidor de contacto 3a Proxy Call Session Control Function (P-CSCF, intermedidario de la función de control de las sesiones de llamada), al servidor de sesión 3b Serving Call Session Control Function (S-CSCF, servidor de la función de control de las sesiones de llamada) y al servidor de abonados 3c Home Subscriber Server (HSS, servidor doméstico de abonados).

La función de los distintos componentes, servidor de contacto 3a, servidor de sesión 3b y servidor de abonados 3c, y con ello también la función del servidor de control 3 y de los generadores de claves de medios 9, se describirá a continuación más en detalle en relación con la figura 3.

La figura 3 muestra un diagrama secuencial del establecimiento de un enlace y una subsiguiente transmisión de datos de medios codificados CMD entre el servidor de medios 5 y el aparato de abonado 1. En el establecimiento del enlace participan el servidor de contacto 3a, el servidor de sesión 3b y el servidor de abonados 3c.

En una primera etapa S1 formula el aparato de abonado 1 una consulta relativa al establecimiento del enlace, denominada también consulta “Sub-Registration (sub-registro”, al servidor de contacto 3a del servidor de control 3. En un IMS según el estándar 3GPP, en el que el servidor de contacto se denomina Proxy Call Session Control Function (P-CSCF), puede utilizarse por ejemplo como protocolo de iniciación de sesión el llamado protocolo de inicio de sesión (Session Initiation Protocol, SIP, según RFC 3261 y RFC 2543) junto con el Session Description Protocol (SDP, protocolo de descripción de la sesión, según RFC 2327). En la consulta, en la etapa S1, se transmiten en particular los datos de identificación ID que caracterizan inequívocamente al aparato de abonado 1. Estos datos de identificación ID están archivados en teléfonos móviles por ejemplo en la llamada tarjeta SIM (Subscriber Identity Module, módulo de identidad de abonado). Los datos de identificación ID se necesitan entonces a continuación para determinar el conjunto de parámetros de codificación K que se utilizan para la codificación del intercambio a continuación de datos de control entre el aparato de abonado 1 y el servidor de control 3. Para transmitir informaciones mientras se determina el conjunto de parámetros de codificación K, puede utilizarse por ejemplo el protocolo de codificación multimedia de Internet Multimedia Internet KEYing (MIKEY, según RFC 3830) dentro del protocolo SIP. Igualmente podría realizarse la transmisión según las descripciones de seguridad (Security Descriptions, SDES, según un proyecto de IETF, Internet Engineering Task Force, grupo de trabajo de ingeniería de Internet).

En una segunda etapa S2 se retransmiten los datos de identificación ID desde el servidor de contacto 3a a través del servidor de sesión 3b al servidor de abonados 3c. El servidor de sesión 3b (en un sistema 3GPP la S-CSCF, dado el caso con apoyo de una llamada Interrogating Call Session Control Function I-CSCF, integrador de la función de control de las sesiones de llamada), sirve para asegurar datos de sesión, por ejemplo para la facturación y en el contexto aquí presentado sólo tiene una importancia marginal. El servidor de abonado 3c dispone de un banco de datos (o bien tiene acceso al mismo), en el que están archivados los datos de identificación ID de aparatos de abonado. El servidor de abonados 3c (Home Subscriber Server en un sistema 3GPP) averigua el número aleatorio R y determina, en base al número aleatorio R y en función de los datos de identificación ID, la clave de datos de control CK y la clave de integridad IK. Por razones de seguridad no se utilizan para determinar la clave los datos de identificación ID directamente, sino una secuencia de números o caracteres asociada en el banco de datos a los datos de identificación ID. Los procedimientos y algoritmos que pueden utilizarse para generar la clave se conocen por las correspondientes especificaciones del sistema 3GPP. El número aleatorio R,

la clave de datos de control CK y la clave de integridad IK forman el conjunto de parámetros de codificación K.

Este conjunto de parámetros de codificación K se envía en una etapa S3 desde el servidor de abonados 3C a su vez a través del servidor de sesión 3b al servidor de contacto 3a. La clave de datos de control CK y la clave de integridad IK están disponibles así a partir de entonces para el servidor de contacto 3a para la codificación de datos de control que se intercambian con el aparato de abonado 1. La clave de datos de control CK se utiliza para la codificación propiamente dicha con un algoritmo de codificación simétrico. Las secuencias enviadas adicionalmente con los datos de control, codificadas con la clave de integridad IK, permiten comprobar la integridad de los datos de control y detectar eventuales intentos de manipulación. Según 3GPP tienen ambas claves una longitud de 128 bits.

En una etapa S4 se envía el número aleatorio R del conjunto de parámetros de codificación K (sin codificar) al aparato de abonado 1. Las claves CK e IK no se transmiten por razones de seguridad, sino que son generadas por el propio aparato de abonado 1, tal como se describirá más tarde.

Además, determina el servidor de contacto 3a en una etapa S5 la clave de medios MK a partir de la clave de datos de control CK y la clave de integridad IK. Por ejemplo puede calcularse la clave de medios MK mediante una combinación O-exclusiva (XOR) de ambas claves CK e IK. La misma es en particular adecuada en el 3GPP, porque ambas claves CK e IK presentan la misma longitud. Alternativamente es posible por ejemplo determinar la clave de medios MK mediante una reproducción irreversiblemente inequívoca de ambas claves CK e IK. Una tal reproducción se denomina también función Hash de una vía. Las funciones Hash de una vía utilizables se conocen por ejemplo como Messenger Digest (MD4, MD5) o Secure Hash Algorithm (SHA, algoritmo Hash seguro). Las funciones Hash de una vía tienen la ventaja de que a partir de una clave de medios MK que se ha llegado a conocer no es posible deducir las claves CK e IK que sirven de base. No obstante, básicamente es adecuada para el cálculo de la clave de medios MK cualquier otra función a partir de la que pueda calcularse una secuencia de claves a partir de una o de ambas claves CK e IK. Entonces no necesita coincidir la longitud de la clave de medios resultante MK con la de las claves CK e IK utilizadas. Además, adicionalmente a las claves CK e IK, pueden incluirse parámetros adicionales en la determinación de la clave de medios MK. La premisa al respecto es solamente que tanto el aparato de abonado 1 como también el servidor de contacto 3a dispongan de estos parámetros. El número aleatorio R o los datos de identificación ID son ejemplos de tales parámetros.

Una vez que el aparato de abonado 1 ha recibido el número aleatorio transmitido en la etapa S4, averigua el aparato de abonado en una etapa S6 a partir del número aleatorio R en función de los datos de identificación ID la clave de datos de control CK y la clave de integridad IK. Esto se realiza de la misma manera que en el servidor de abonados 3c, con lo que existen idénticas claves IK y CK en el servidor de control 3 y en el aparato de abonado 1. La secuencia de números o caracteres utilizada por razones de seguridad para determinar la clave en lugar de los propios datos de identificación ID, está memorizada en el aparato de abonado usualmente en la tarjeta SIM.

Análogamente a en la etapa S5, se genera ahora en el aparato de abonado 1 en una etapa S7, a partir de las claves CK e IK, la clave de medios MK.

En base al número aleatorio R determina el aparato de abonado 1 además una respuesta de autentificación, con la que en una etapa S8 se envía una segunda consulta como siguiente etapa del establecimiento del enlace por ejemplo a través del Session Initiation Protocol (SIP) al servidor de control 3a.

Esta segunda consulta se retransmite en una etapa S9 al servidor de sesión 3b, que comprueba la respuesta de autentificación del aparato de abonado 1 y, si el resultado es positivo, registra la sesión como iniciada con éxito y envía en una etapa S10 una secuencia de confirmación de retorno al servidor de contacto 3a. Basándose en el protocolo de transporte de hipertexto Hypertext Transport Protocol (HTTP) se utiliza también en el SIP un aviso de estado (status) "200 OK" como confirmación positiva. En una etapa S11 se retransmite la secuencia de confirmación al aparato de abonado 1.

En este punto ha finalizado el establecimiento del enlace y de la sesión y puede iniciarse la transmisión de datos útiles. Para el procedimiento se supone que en este punto también ha finalizado la determinación de la clave de medios MK en las etapas S5 y S7 tanto en el servidor de contacto 3a como también en el aparato de abonado 1.

En una etapa S12 fórmula el aparato de abonado 1 una consulta para transmitir los datos de medios deseados al servidor de contacto 3a. En el Session Initiation Protocol (SIP) está prevista para una tal consulta la secuencia "Invite" (invitar, con la que pueden traerse datos de medios MD del servidor de medios 5, pudiendo encontrarse los datos ya en el servidor de medios 5 o bien pueden ser datos de conversación que deben intercambiarse a través del servidor de medios 5 con otro aparato de abonado. En el protocolo SIP está previsto que con la consulta pueda enviarse un contexto de codificación, que por ejemplo indica el algoritmo de codificación a utilizar. El contexto de codificación no incluye la clave de

medios MK, aun cuando esto sería posible según el protocolo SIP, ya que la clave de medios MK existe ya en el procedimiento correspondiente a la invención en el servidor de control 3.

En una etapa S13 se retransmite la consulta "Invite", pero sin contexto de codificación, desde el servidor de contacto 3a al servidor de sesión 3b. El servidor de sesión 3b protocoliza la consulta y averigua si la consulta es procedente, es decir, por ejemplo si el aparato de abonado 1 está autorizado para el acceso a los datos de medios MD consultados o no. En el caso de que la consulta sea procedente, envía el servidor de sesión 3b en una etapa S16 el aviso de estado "200 OK" como confirmación positiva de retorno al servidor de contacto 3a. En el caso de que se consulten datos de medios MD que ya no existan, sino una conversación con otro aparato de abonado, toma contacto el servidor de sesión 3b tras la etapa S13 primeramente en una etapa S14 con un correspondiente servidor de sesión 3b*, que es competente para el otro aparato de abonado.

En una etapa S15 recibe el servidor de sesión 3b del interlocutor un aviso de estado como respuesta, que a continuación se retransmite en la etapa S16.

Una vez que el servidor de contacto 3a ha recibido del servidor de sesión 3b el aviso de retorno, envía el mismo el aviso de estado recibido en una etapa S18 al aparato de abonado 1.

Si la consulta era procedente y el aviso de retorno ha sido positivo, transmite el servidor de contacto 3a en una etapa S18 tanto el contexto de codificación como también la clave de medios MK al servidor de medios 5. Además de ello, se transmiten otras informaciones que caracterizan los datos de medios MD a transmitir. Puesto que esta transferencia se realiza a través de la red núcleo 4, que en general no es pública, no es necesaria aquí básicamente ninguna otra medida de seguridad para proteger la clave de medios MK. Si como medida de seguridad adicional se desea, o en el caso de que la red núcleo 4 sea total o parcialmente pública, puede evidentemente realizarse la transferencia también codificada.

El servidor de medios 5 codifica a continuación los datos de medios MD con la clave de medios MK en el contexto de codificación consultado, es decir, por ejemplo utilizando el algoritmo de codificación indicado. Los datos de medios codificados CMD recibidos se envían en una etapa final S19 al aparato de abonado 1.

Puesto que la red de medios 6 usualmente es de conmutación por paquetes, es procedente no codificar los datos de medios MD básicamente como un conjunto y transmitirlos a continuación por paquetes, sino codificar en cada caso los paquetes individuales. En el aparato de abonado 1 pueden decodificarse los datos de medios codificados CMD recibidos, ya que el aparato de abonado 1 dispone del contexto de codificación (prescrito por el mismo) y también de la clave de medios MK necesaria (calculada en la etapa S7).

Durante la transmisión de los datos de medios codificados CMD pueden intercambiarse en paralelo en el tiempo ya otros datos de control entre el aparato de abonado 1 y el servidor de control 3. Estos datos de control pueden servir por ejemplo para comprobar el correcto desarrollo de la transmisión o referirse a otras consultas. Entonces puede llegarse a acordar nuevas claves CK e IK. Es ventajoso en un tal caso calcular también de nuevo la clave de medios MK, ya que un mecanismo de codificación es tanto más seguro cuanto más corta sea la clave que se utiliza. Desde luego cuando se calcula de nuevo una clave de medios MK puede llegarse a problemas de sincronización cuando el servidor de medios 5 y el aparato de abonado 1 no dispongan a la vez de la nueva clave. No obstante, en un caso así se recurre a mecanismos de corrección y tratamiento de faltas ya conocidos y previstos en el 3GPP. Un paquete decodificado por el servidor de medios 5 con una clave de medios MK que no exista en el aparato de abonado 1, se catalogaría por el aparato de abonado 1 como corrupta y bien se rechazaría (en datos de conversación) o bien la solicitaría de nuevo el aparato de abonado 1 del servidor de control 3a.

REIVINDICACIONES

1. Procedimiento para codificar y decodificar datos de medios (MD, CMD), que presenta las etapas:

- transmisión de una consulta desde un aparato de abonado (1) a través de una red de control (2) hasta un servidor de control (3) para determinar un conjunto de parámetros de codificación (K) para datos de control, incluyendo la consulta datos de identificación (ID) del aparato de abonado (1),

- determinación del conjunto de parámetros de codificación (K) para datos de control mediante el servidor de control (3), que incluye un número aleatorio (R), una clave de datos de control (CK) y una clave de integridad (IK), dependiendo la clave de datos de control (CK) y la clave de integridad (IK) del número aleatorio (R) y de los datos de identificación (ID),

- generación de una clave de medios (MK) en función de la clave de datos de control (CK) y de la clave de integridad (IK) mediante el servidor de control (3),

- transmisión de la clave de medios (MK) desde el servidor de control (3) a un servidor de medios (5) a través de una red núcleo (4),

- codificación de datos de medios (MD) no codificados mediante el servidor de medios (5) utilizando la clave de medios (MK) para su envío a través de una red de datos (6) al aparato de abonado (1) y/o

- decodificación de datos de medios codificados (CMD) enviados por un aparato de abonado (1) y recibidos a través de la red de datos (6) mediante el servidor de medios (5) utilizando la clave de medios de (MK).

2. Procedimiento según la reivindicación 1,

en el que, adicionalmente a la clave de medios (MK), se transmiten otros parámetros de codificación, en particular relativos al algoritmo de codificación a utilizar, desde el servidor de control (3) a través de la red núcleo (4) al servidor de medios (5)

3. Procedimiento según la reivindicación 2,

en el que se fijan los otros parámetros de codificación previamente en el aparato de abonado (1) y se transmiten al servidor de control (3).

4. Procedimiento según la reivindicación 2,

en el que los otros parámetros de codificación se acuerdan entre el aparato de abonado (1) y el servidor de control (3).

5. Procedimiento para codificar y decodificar datos de medios (MD, CMD) que presenta las etapas:

- transmisión de una consulta desde un aparato de abonado (1) a través de una red de control (2) hasta un servidor de control (3) para determinar un conjunto de parámetros de codificación (K) para datos de control, incluyendo la consulta datos de identificación (ID) del aparato de abonado (1),

- determinación del conjunto de parámetros de codificación (K) para datos de control mediante el servidor de control (3), que incluye un número aleatorio (R),

- transmisión del número aleatorio desde el servidor de control (3) al aparato de abonado (1),

- determinación de una clave de datos de control (CK) y una clave de integridad (IK) en función del número aleatorio (R) y de los datos de identificación (ID) por parte del aparato de abonado (1),

- generación de una clave de medios (MK) en función de la clave de datos de control (CK) y de la clave de integridad (IK) mediante el aparato de abonado (1),

- decodificación de datos de medios codificados (CMD) enviados por un servidor de medios (5) recibidos a través de una red de datos (6) mediante el aparato de abonado (1) utilizando la clave de medios (MK) y/o

- codificación de datos de medios (MD) no codificados mediante el aparato de abonado (1) utilizando la clave de medios (MK) para su envío a través de la red de datos (6) al servidor de medios (5).

6. Procedimiento según una de las reivindicaciones 1 a 5,

en el que la clave de medios (MK) se forma mediante una combinación O-exclusiva a partir de la clave de datos de control (CK) y de la clave de integridad (IK),

7. Procedimiento una de las reivindicaciones 1 a 5,

en el que la clave de medios (MK) se forma mediante una función Hash de una vía a partir de la clave de datos de control (CK) y de la clave de integridad (IK).

8. Procedimiento según una de las reivindicaciones 1 a 7,

en el que la clave de medios (MK) se utiliza directamente para la codificación y decodificación.

9. Procedimiento según una de las reivindicaciones 1 a 7,

en el que, en función de la clave de medios (MK), se determina una clave adicional, que se utiliza para la codificación y decodificación.

10. Servidor de control (3) de un sistema de comunicaciones, que presenta

- una primera interfaz hacia una red de control (2),
- una segunda interfaz hacia una red núcleo (4),

en el que

- el servidor de control (3) puede unirse a través de la primera interfaz y la red de control (2) con un aparato de abonado (1) y a través de la segunda interfaz y la red núcleo (4) con un servidor de medios (5) y

en el que el servidor de control (3) está equipado para

- recibir datos de identificación (ID) del aparato de abonado (1),
- determinar un conjunto de parámetros de codificación (K) para datos de control, incluyendo los parámetros de codificación (K) un número aleatorio (R) y en función del número aleatorio (R) y de los datos de identificación (ID), una clave de datos de control (CK) y una clave de integridad (IK),
- generar una clave de medios (MK) en función de la clave de datos de control (CK) y de la clave de integridad (IK) y
- transmitir la clave de medios (MK) a través de la red núcleo (4) al servidor de medios (5).

11. Aparato de abonado (1) para su utilización en un sistema de comunicaciones, que presenta

- una primera interfaz hacia una red de control (2),
- una segunda interfaz hacia una red de medios (4),

en el que

- el aparato de abonado (1) puede conectarse a través de la primera interfaz y de la red de control (2) para intercambiar datos de control con un servidor de control (3) y a través de la segunda interfaz y la red de medios (4) para el intercambio de datos de medios (MD, CMD) con un servidor de medios (5) y

estando equipado el aparato de abonado (1) para

- enviar datos de identificación (ID) al servidor de control,
- recibir como respuesta un número aleatorio (R),
- generar una clave de datos de control (CK) y una clave de integridad (IK) en función del número aleatorio (R) y los datos de identificación (ID), sirviendo la clave de datos de control (CK) y la clave de integridad (IK) para codificar y decodificar los datos de control y
- generar una clave de medios (MK) en función de la clave de datos de control (CK) y de la clave de integridad (IK), sirviendo la clave de medios (MK) para codificar y decodificar los datos de medios (MD, CMD).

12. Producto de programa de computadora con código de programa para ejecutar un programa de computadora en una o varias computadoras de un sistema de comunicaciones,

caracterizado porque cuando se ejecuta el código de programa, se ejecuta un procedimiento según una de las reivindicaciones 1 a 7.

FIG 1

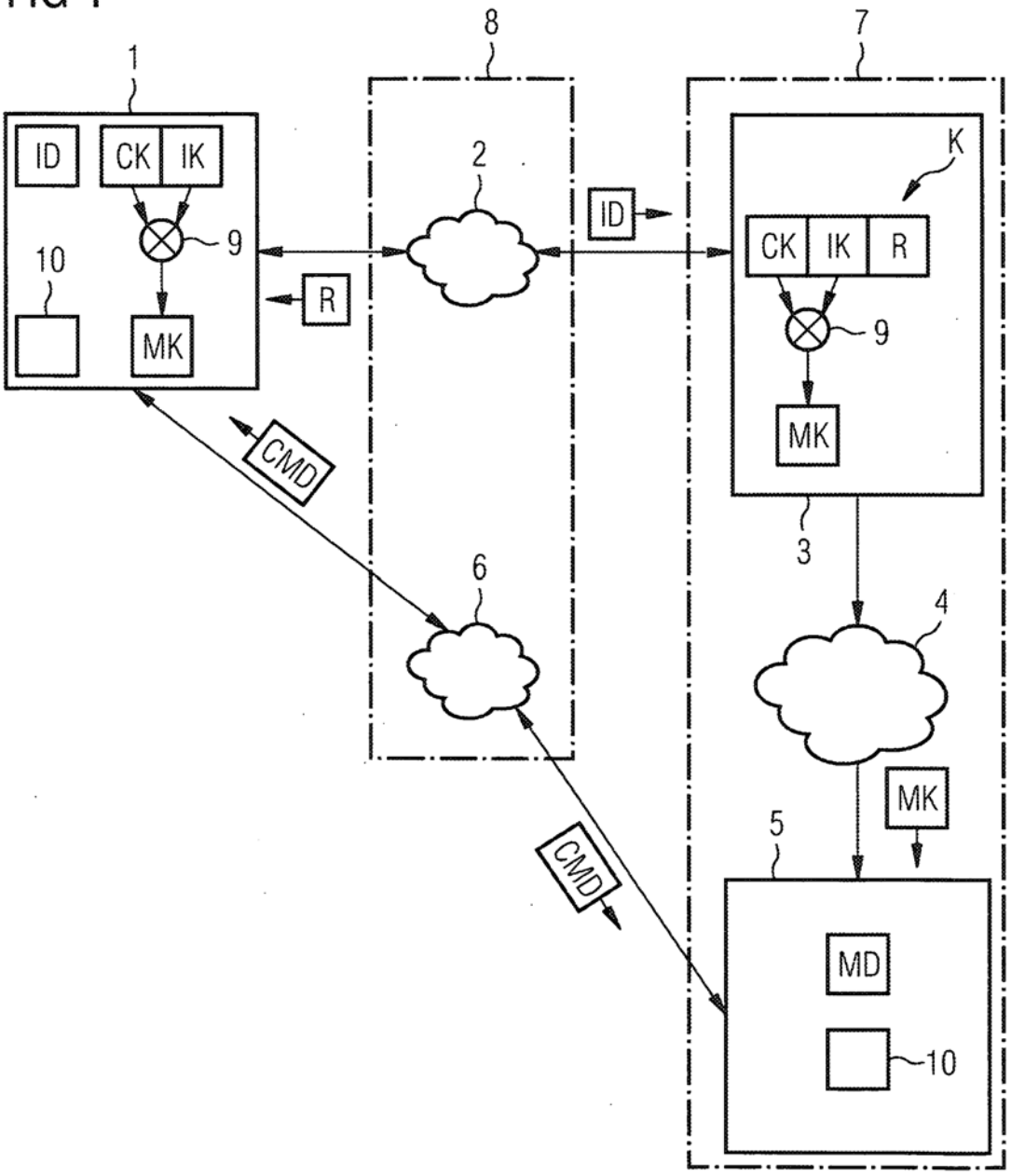


FIG 2

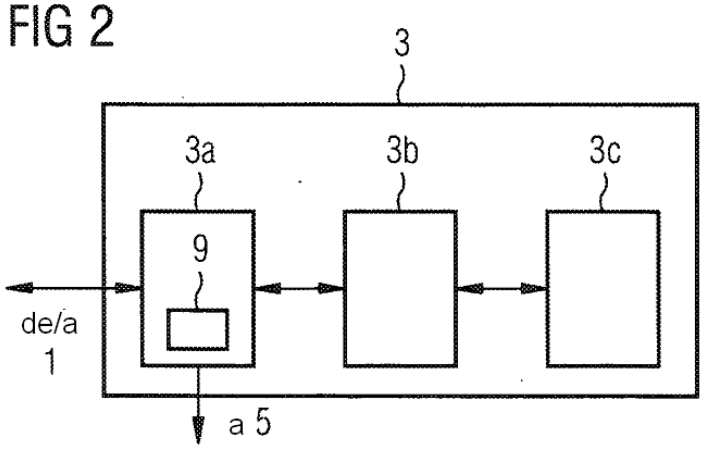
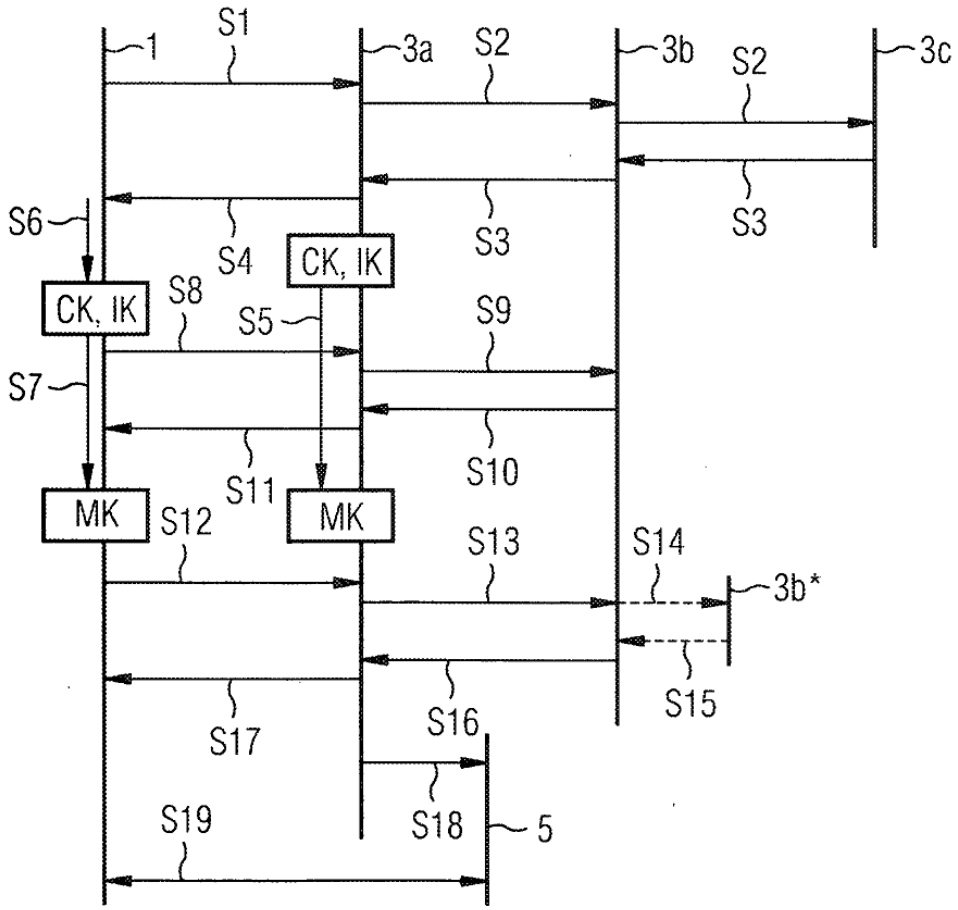

3
3a
3b
3c
9
de/a
1
a 5

FIG 3


1
S1
3a
S2
3b
S2
3c
S3
S3
S6
S4
CK, IK
CK, IK
S8
S5
S9
S7
S10
S11
MK
S12
MK
S13
S14
3b*
S15
S17
S16
S18
5
S19