(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 479 115**

(51) Int. CI.:

***H04N 21/266*** (2011.01)
***H04N 21/418*** (2011.01)
***H04N 21/6334*** (2011.01)
***H04N 21/643*** (2011.01)
***H04L 29/06*** (2006.01)
***H04N 7/167*** (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.09.2008 E 08164940 (2)**

(97) Fecha y número de publicación de la concesión europea: **23.04.2014 EP 2061244**

(54) Título: **Protección de contenido de difusión con distribución de clave mediante la red de telecomunicaciones**

(30) Prioridad:

**27.09.2007 GB 0718826**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**23.07.2014**

(73) Titular/es:

**VODAFONE GROUP PLC (100.0%)**
**GROUP LEGAL (PATENTS), THE CONNECTION**
**NEWBURY, BERKSHIRE RG14 2FN, GB**

(72) Inventor/es:

**WRIGHT, TIMOTHY y**
**PRIESTLEY, MARK**

(74) Agente/Representante:

**DE ELZABURU MÁRQUEZ, Alberto**

## DESCRIPCIÓN

Protección de contenido de difusión con distribución de clave mediante la red de telecomunicaciones

La presente invención se refiere a un método de controlar el uso, por parte de un terminal de usuario registrado en una red de telecomunicaciones, de contenido emitido por un medio de emisión y codificado mediante una clave. La presente invención se refiere también a un aparato para controlar el uso del contenido emitido.

La emisión de TV mediante telefonía móvil sobre una portadora de emisión (por ejemplo DVB-H) tiene problemas de seguridad que no existen cuando el mismo contenido es proporcionado sobre una portadora de punto a punto (por ejemplo, transmitido en tiempo real sobre una red 3G). Sobre una portadora de emisión el contenido es emitido y así puede en principio ser recibido por cualquiera con el tipo correcto de receptor. No obstante, para poder tarificar el contenido emitido, el proveedor de servicio necesita poder controlar quién puede y quién no puede acceder a los servicios. Esto se consigue típicamente codificando el contenido emitido y proporcionando mecanismos para legitimar a abonados para obtener las claves necesarias para descodificar ese contenido. El término genérico para estos mecanismos y la codificación del canal es la protección de servicio. Existen varias soluciones de protección de servicio estandarizadas.

Generalmente la protección de servicio utiliza una jerarquía de claves en la cual cada capa de claves es utilizada para proteger el contenido o las claves de la capa inferior. En este documento los términos “codificar” y “codificado” se utilizan con el significado de que una clave se utiliza directamente para codificar el contenido en cuestión o una clave derivada de la clave referenciada se utiliza para codificar el contenido en cuestión. La integridad y/o la autenticidad del contenido que se está codificando pueden ser proporcionadas por otros mecanismos criptográficos.

El contenido es codificado utilizando Claves de Codificación de Tráfico (TEKS – Traffic Encryption Keys, en inglés), junto con un protocolo de protección estandarizado (por ejemplo, IPsec, SRTP), antes de ser emitido. Las TEKs cambian frecuentemente (cada minuto o menos) para impedir un ataque basado en el acceso a las TEKs dentro de un dispositivo y la redistribución de las TEKs a receptores no autorizados.

Los abonados legítimos no pueden descodificar el canal emitido sin acceder a las TEKs. Las propias TEKs son codificadas utilizando claves de Codificación de Servicio (SEKs – Service Encryption Keys, en inglés). Las TEKs codificadas son enviadas, junto con el contenido codificado, sobre el canal de emisión. En los sistemas de TV digital terrestre y por satélite estas TEKs protegidas se denominan Mensajes de Control de Derechos (ECMs – Entitlement Control Messages, en inglés). En las especificaciones OMA BCAST estas TEKs se denominan “mensajes de flujo de claves” o Mensajes de Clave de Corto Plazo (STKMs – Short Term Key Messages, en inglés).

Los abonados legítimos no pueden extraer la TEK de los mensajes del flujo de claves sin acceder a la Clave de Codificación de Servicio (SEK – Service Encryption Key, en inglés). Sólo los abonados legítimos deben tener acceso a la Clave de Codificación de Servicio.

Un proveedor de servicio normalmente asignará una SEK separada para cada canal que emite. Si un usuario se suscribe a uno o a más canales requerirá una SEK para cada canal al cual se suscribe.

Las Claves de Codificación de Servicio (SEKs – Service Encryption Keys, en inglés) pueden tener vidas útiles de decenas de minutos a meses, aunque por definición deben tener una vida significativamente mayor que las TEKs a las que protegen. Cambiando la vida útil de una SEK el Proveedor de Servicios puede controlar la duración de suscripción que puede ser ofrecida a sus usuarios (aunque son posibles otros mecanismos). En algunos casos las SEKs pueden tener una vida útil igual a la de un único programa, por ejemplo, una película de pago por visión o un evento deportivo. En tal caso las SEKs se denominan a menudo “Claves de Codificación de Programa” o PEKs (Programme Encryption Keys, en inglés). Algunas soluciones, tales como el perfil 18Crypt/DRM, permiten la anidación de PEKs y SEKs, por ejemplo las PEKs están codificadas utilizando SEKs.

Las SEKs son normalmente enviadas sobre un canal de punto a punto y están codificadas utilizando otra clave, denominada en esta memoria “Clave de Usuario”. La Clave de Usuario es única para un abonado particular y puede ser la clave del nivel más alto dentro de la jerarquía de claves de protección del servicio. Las especificaciones del perfil DVB-H IPDC 18Crypt y del perfil OMA BCAST DRM utilizan Objetos de Derechos (ROs – Right Objects, en inglés) de Versión 2 de OMA DRM [OMA DRM] para enviar de manera segura la SEK a terminales individuales. El Perfil de Tarjeta Inteligente de OMA BCAST utiliza el protocolo MIKEY [IETF MIKEY] para enviar de manera segura la SEK al USIM del usuario (a través del terminal de usuario).

En ambos casos estos mensajes se denominan mensajes de Clave de Largo Plazo (LTKMs – Long Term Key Messages, en inglés).

Convencionalmente, las SEKs, y cualquier clave derivada de las SEKs para codificar las TEKs son claves simétricas. Esto significa que la misma clave es utilizada para codificar la TEK igual que se utiliza para descodificar la TEK.

Una revisión de los problemas de la protección de servicios convencional anterior es proporcionada en un artículo por uno de los inventores – “Security consideration for broadcast systems”, Information Security Technical Report, Elsevier Advanced Technology, vol. 11, nº 3, 1 de Enero de 2006.

Sugerencias específicas para optimizar la prestación de servicios de transporte en MBMS se establecen en el documento de explicación de estándares ”N to N relationship between User Services and Transport Services” [BORRADOR DEL 3GPP: S3-040489_MBMS_USER_TRANSPORT_RELATIONV2, PROYECTO DE COLABORACIÓN DE 3ª GENERACIÓN (3GPP), 29 de Junio de 2004]. Este documento específicamente requiere que aunque dos servicios de usuario de MBMS pueden ambos utilizar al menos un servicio de transporte, la clave del servicio para ese servicio de transporte compartido no debe ser utilizada para cualquier otro servicio de transporte.

El uso combinado tanto de codificación de claves asimétrica como de codificación de claves simétrica se conoce del documento “Pretty Good Privacy” que puede encontrarse en Wikipedia, por ejemplo la versión de 22.09.2007.

Las Plataformas de Protección de Servicios deben soportar un generador de STKM y un generador de LTKM. Varios operadores de red de telefonía móvil (MNOs – Mobile Network Operators, en inglés) pueden por razones de economía compartir elementos de una Plataforma de Protección de Servicios, por ejemplo, el generador de STKM. Es menos probable que los MNOs compartan un generador de LTKM puesto que éste genera mensajes que son específicamente para sus abonados y son típicamente enviados sobre la red celular y ninguna portadora de emisión.

Un problema con que los MNOs compartan el generador de STKM es que el generador de STKM necesita acceder a la SEK con el fin de generar los STKMs (por ejemplo, las TEKs codificadas mediante las SEKs). No obstante, las SEKs son específicas para un operador, y son claves muy valiosas. La liberación de las SEKs para el generador de STKM compartido en la plataforma de emisión es un riesgo de seguridad para los MNOs. Si la SEK resultase conocida para una entidad no autorizada, esa entidad podría descodificar el contenido emitido protegido utilizando la SEK para extraer la TEK del STKM y utilizar entonces la TEK extraída para descodificar el contenido protegido.

De acuerdo con un primer aspecto de la presente invención, se proporciona un método de controlar el uso, tal como se describe en la reivindicación 1.

La comunicación de punto a punto entre la red de telecomunicaciones y el terminal de usuario convenientemente envía la tercera clave privada privada codificada mediante otra clave.

El medio de emisión puede ser compartido por las redes telecomunicaciones.

Ventajosamente, el medio de emisión puede transmitir la primera clave al medio de codificación, transmitiendo el medio de codificación la primera clave codificada al medio de emisión, para la emisión directa al terminal de usuario.

El terminal de usuario preferiblemente incluye medios de autenticación para almacenar datos de autenticación para la autenticación del terminal de usuario con la red de telecomunicaciones.

Además, el terminal de usuario puede incluir un módulo seguro para almacenar la clave tercera privada.

Alternativa o adicionalmente, el terminal de usuario puede incluir medios para recibir el contenido codificado emitido y la primera clave codificada emitida, y para separar el contenido codificado de la primera clave codificada.

El terminal de usuario puede incluir una aplicación para acceder a la tercera clave privada, para recibir la primera clave codificada y para derivar la primera clave de la misma con el fin de permitir el consumo del contenido.

El contenido es preferiblemente emitido por al menos uno de DVH-H y DVB-T.

La red de telecomunicaciones preferiblemente comprende una red de telecomunicaciones de telefonía móvil o celular, tal como GSM, GPRS, UMTS o 4G / SAE / LTE.

La correspondiente clave puede permitir la extracción de la primera clave, lo cual a su vez permite la descodificación del contenido emitido.

En la realización la primera clave es una Clave de Codificación de Tráfico (TEK - Traffic Encryption Key, en inglés). La segunda clave y la correspondiente clave son partes respectivas de un par de claves pública / privada de la Clave de Codificación de Servicio (SEK – Service Encryption Key, en inglés) (SEK_pub / SEK_priv).

La primera clave / TEK puede ser directamente codificada mediante la segunda clave / SEK_pub o la segunda clave / SEK_pub puede ser utilizada para derivar otra clave que es utilizada para codificar la primera clave / TEK. Si la primera clave / TEK es codificada mediante una clave derivada de la segunda clave / SEK, entonces el terminal debe llevar a cabo la correspondiente función de derivación utilizando la correspondiente clave / SEK_priv para obtener la clave necesaria para descodificar la TEK.

En la realización la primera clave / TEK, codificada mediante la segunda clave / SEK_pub, y los datos relativos a las claves y servicios a los que protegen, comprende un Mensaje de Clave de Corto Plazo (STKM – Short Term Key Message, en inglés). Como el STKM es generado codificando la primera clave / TEK con la segunda clave / SEK_pub y combinando la TEK codificada mediante la SEK con datos relativos a las claves y servicios a los que protegen, el generador de STKM puede ser compartido entre una pluralidad de Proveedores de Servicios (por ejemplo, Operadores de Red de Telefonía Móvil) sin un significativo riesgo para la seguridad, en contraste con la técnica anterior. Incluso si la segunda clave / SEK_pub se conociese, esto no permitiría la extracción no autorizada de la primera clave / TEK del STKM. La primera clave / TEK sólo puede ser extraída del STKM por una entidad que tenga la correspondiente clave / SEK_priv. Como la correspondiente clave / SEK_priv es transmitida mediante una comunicación de punto a punto desde el Proveedor de Servicios al terminal de telefonía móvil, es menos probable que éste sea interceptado. Esto es especialmente cierto en la realización en la que la correspondiente clave / SEK_priv es enviada protegida por una Clave de Usuario (UK – User Key, en inglés) compartida entre el Proveedor de Servicios y el terminal de usuario - preferiblemente en un modo seguro del mismo. La UK puede ser preconfigurada en el terminal de usuario durante la fabricación, en una tarjeta inteligente para su inserción en el terminal de usuario, o generada “sobre la marcha” utilizando información proporcionada previamente durante la fabricación.

La realización proporciona significativas mejoras en la seguridad utilizando un par de claves pública / privada para la SEK, en contraste con las SEKs simétricas de la técnica anterior descrita anteriormente. La realización permite que el medio de emisión y un generador de STKM sean compartidos entre una pluralidad de proveedores de servicios sin comprometer significativamente la seguridad. Tal disposición de recursos compartidos no era posible con la disposición de la técnica anterior, sin comprometer la seguridad.

En la realización la correspondiente clave / SEK_priv permite que la primera clave / TEK del STKM sea descodificada. El módulo seguro en el terminal de telefonía móvil es entonces capaz de utilizar la primera clave / TEK codificada requerida para descodificar el contenido codificado recibido en el canal de emisión y para reproducir ese contenido en el terminal de telefonía móvil.

En la realización la seguridad puede ser también mejorada haciendo segura la correspondiente clave / SEK_priv en el módulo seguro. El módulo seguro puede ser implementado por el terminal de telefonía móvil, por ejemplo, o puede ser implementado en una tarjeta inteligente tal como una Tarjeta de Circuitos Integrados Universal (UICC – Universal Integrated Circuit Card, en inglés) que puede opcionalmente también implementar un Módulo de Identidad de Abonado (SIM – Subscriber Identity Module, en inglés) o un SIM Universal (USIM – Universal SIM, en inglés) u otra aplicación. Las tarjetas inteligentes son elementos de hardware de seguridad altamente seguros, que son fiables para los Operadores de Redes de Telefonía Móvil. El riesgo de que la correspondiente clave / SEK_priv sea obtenida ilegítimamente de la tarjeta inteligente es muy pequeño.

De acuerdo con un segundo aspecto de la presente invención, se proporciona un sistema para controlar el uso, tal como se describe en la reivindicación 7.

La comunicación de punto a punto entre la red de telecomunicaciones y el terminal de usuario puede convenientemente enviar la tercera clave privada codificada mediante otra clave.

El medio de emisión puede ser compartido por las redes de telecomunicaciones.

El medio de emisión puede transmitir la primera clave al medio de codificación, siendo el medio de codificación operable para codificar la primera clave utilizando la segunda clave pública.

El sistema puede convenientemente incluir el propio terminal de usuario. En este caso, el terminal de usuario preferiblemente incluye un medio de autenticación para almacenar datos de autenticación para la autenticación del terminal de usuario con la red de telecomunicaciones.

El terminal de usuario puede incluir un módulo seguro para almacenar la tercera clave privada. El módulo seguro puede ser implementado en hardware o software.

Alternativa o adicionalmente, el terminal de usuario puede incluir un medio para recibir el contenido codificado emitido y la primera clave codificada emitida y para separar el contenido codificado de la primera clave codificada.

El terminal de usuario preferiblemente incluye una aplicación para acceder a la correspondiente clave y para recibir la primera clave codificada, y para derivar la primera clave de la misma con el fin de permitir el consumo del contenido.

El contenido puede ventajosamente ser emitido por al menos uno de DVH-H y DVB-T.

La red de telecomunicaciones puede comprender una red de telefonía móvil o celular, tal como GSM, GPRS, UMTS ó 4G / SAE / LTE.

La red de telecomunicaciones puede ser una red celular GSM, GPRS o UMTS, por ejemplo.

Para una mejor comprensión de la presente invención se describirá ahora una realización a modo de ejemplo, con referencia al dibujo que se acompaña, la única figura del cual muestra esquemáticamente los elementos de un sistema de emisión de acuerdo con una realización de la invención.

El terminal de telefonía móvil 1 incluye una pantalla 2 y un teclado 4. El terminal 1 está registrado con un Operador de Red de Telefonía Móvil (MNO – Mobile Network Operator, en inglés) 3 (u otro proveedor de servicios) y es proporcionado con el módulo seguro 5. El módulo seguro 5 es implementado en una tarjeta inteligente en la realización, pero esto no es esencial. Opcionalmente, la tarjeta inteligente puede incluir un Módulo de Identidad de Abonado (SIM – Subscriber Identity Module, en inglés, o USIM, que puede permitir que el MNO 3 autentique al usuario del terminal 1 utilizando autenticación de GSM o de UMTS. El módulo seguro 5 permite al proveedor de servicios compartir de manera segura una clave específica para el usuario, la “Clave de Usuario” (UK – User Key, en inglés), con el módulo seguro 5. La Clave de Usuario puede ser proporcionada previamente durante la fabricación del módulo seguro 5 ó generada “sobre la marcha” utilizando información proporcionada previamente durante la fabricación.

Si el módulo seguro 5 comprende un SIM o USIM, o si un SIM / USIM es proporcionado en algún otro lugar para su uso por el terminal, información de autenticación puede ser almacenada en el SIM / USIM bajo el control del MNO 3. El propio MNO 3 almacena detalles de cada uno de los SIM / USIM emitidos bajo su control. En operación de MNO 3, el terminal 1 es autenticado (por ejemplo, cuando el usuario activa el terminal en la red con el fin de hacer o recibir llamadas) por la red enviando un desafío al terminal 1 que incorpora el SIM / USIM en respuesta al cual el SIM / USIM calcula una respuesta (que depende de la información predeterminada del SIM / USIM guardada en el medio de autenticación 5 – típicamente un algoritmo de autenticación y una clave única Ki) y lo transmite de vuelta al MNO 3. El MNO 3 incluye un procesador de autenticación que genera el desafío y que recibe la respuesta del terminal 1. Utilizando información previamente almacenada relativa al contenido del medio de autenticación 5 de SIM / USIM relevante, el procesador de autenticación calcula el valor esperado de la respuesta del terminal 1 de telefonía móvil. Si la respuesta recibida coincide con la respuesta calculada esperada, el SIM / USIM y el terminal de telefonía móvil asociado son considerados como autenticados. El SIM / USIM utilizado por el terminal 1 puede ser un SIM del tipo definido en las especificaciones de los estándares de GSM o UMTS, o puede ser una simulación de un SIM – esto es, software o hardware que lleva a cabo una función correspondiente a la del SIM. El SIM puede estar de acuerdo con la disposición descrita en el documento WO-A-2004 036513.

El MNO 3 comprende un generador o almacén de Claves de Usuario (UK – User Key, en inglés), que es operable para generar u obtener la Clave de Usuario para cada usuario. La Clave de Usuario del usuario es almacenada en el medio de autenticación 5 del módulo seguro en el almacén 39.

El terminal 1 es operable para recibir contenido emitido, tal como contenido emitido mediante DVB-H. El contenido emitido puede también ser recibido por otros terminales, tales como el terminal 1’. La plataforma de emisión 7 recibe el contenido 9, por ejemplo, video, de un proveedor de contenidos (no mostrado). La plataforma de emisión 7 comprende un codificador 11 de contenido que es operable para codificar el contenido 9 utilizando una Clave de Codificación de Tráfico (TEK - Traffic Encryption Key, en inglés) generada por el generador de TEK 12. La plataforma de emisión 7 es operable para transmitir el contenido 13 codificado al terminal 1 de telefonía móvil. Para facilitar la descodificación del contenido 13 codificado por parte del terminal 1 de telefonía móvil, la plataforma de emisión 7 también emite mensajes de Clave de Corto Plazo (STKMs – Short Term Key Messages, en inglés) 15 que incluyen las TEKs. El STKM 15 incluye la TEK en forma codificada. La TEK es codificada mediante una Clave de Codificación de Servicios (SEK – Service Encryption Key, en inglés). De acuerdo con una característica importante de la realización, la SEK es utilizada para codificar la TEK es la parte pública de un par de claves pública / privada.

El MNO 3 incluye un generador de SEK 17 que es operable para generar el par de claves pública y privada (SEK_pub y SEK-priv).

Cuando el par de claves pública y privada SEK es generado por el generador de SEK 17 en el MNO 3, además de un mensaje 27 de clave pública que es enviado a un generador de STKM 21, la correspondiente clave privada es pasada al generador de LTKM 41. El generador de LTKM 41 genera LTKMs 43 que comprenden la clave privada protegida por la Clave de Usuario (UK – User Key, en inglés) para el terminal 1 de telefonía móvil. El LTKM 43 es transmitido mediante un canal de punto a punto. Esto es, el LTKM 43 es transmitido sólo al terminal 1 de telefonía móvil y no es emitido a una multiplicidad de terminales. Por ejemplo, el LTKM puede ser transmitido mediante SMS, pulsación de WAP o mediante cualquier otro mecanismo conveniente, tal como sobre una portadora de IP.

El terminal 1 de telefonía móvil incluye un procesador 37 de mensaje en el módulo seguro 5 para procesar el mensaje LTKM 43. A la recepción del LTKM 43 por el terminal 1 de telefonía móvil, el terminal 1 de telefonía móvil pasa el LTKM 43 al procesador de mensajes 37. El procesador de mensajes 37 obtiene la Clave de Usuario (UK – User Key, en inglés) de la ubicación de almacenamiento 39. La Clave de Usuario obtenida del almacén 39 del módulo seguro 5 permite la extracción de la clave privada (SEK_priv) del LTKM 43. La clave privada es a continuación almacenada en el almacén 44 en el módulo seguro 5.

Cuando la plataforma de emisión 7 desea emitir un STKM 15, la plataforma de emisión emite una solicitud de STKM 19 al generador de STKM 21. La solicitud de STKM 19 incluye la TEK de la plataforma de emisión 7 para ser incluida en el STKM. A la recepción de la solicitud de STKM 19, el generador de STKM 21 determina si tiene una clave pública SEK (SEK_pub) apropiada almacenada en el almacén de claves públicas 23 con el fin de generar el STKM. Si se determina que la clave pública SEK relevante no está presente en el almacén de claves públicas 23, el generador de STKM 21 emite una solicitud de SEK 25 al MNO 3. El generador de SEK 17 del MNO 3 genera a continuación un par de SEK pública y SEK privada de la manera descrita anteriormente. La clave pública SEK (SEK_pub) generada por el generador de SEK 17 ó almacenada en el almacén de claves públicas 23 es transmitida al generador de STKM 21 en el mensaje 27. La clave privada SEK (SEK_priv) generada es almacenada en el almacén de claves privadas 29 en el MNO 3. La clave privada es transmitida al terminal 1 de telefonía móvil y almacenada en el almacén 44 en la manera descrita anteriormente.

A la recepción del mensaje 27, el generador de STKM 21 almacena la clave pública SEK en el almacén de claves públicas 23. Como el generador de STKM 21 ahora tiene la clave pública apropiada para generar el STKM en respuesta a la solicitud de STKM 19 recibida desde la plataforma de emisión 7. El generador de STKM 21 recibe a continuación la clave pública relevante del almacén de claves públicas 23 y genera el STKM 33, que es transmitido a la plataforma de emisión 7. La plataforma de emisión 7 a continuación transmite el STKM 33 al terminal 1 de telefonía móvil en el STKM 15.

El terminal 1 de telefonía móvil incluye un filtro o desmultiplexador 35 que recibe datos desde la plataforma de emisión 7 y separa el STKM 15 del contenido codificado 13 emitido.

Cuando el STKM 15 es extraído de los datos emitidos recibidos por el terminal 1 de telefonía móvil por el filtro / desmultiplexador 35, el STKM es pasado al procesador de mensajes 37, que es también operable para procesar el mensaje de STKM 15. El contenido extraído es pasado al módulo de descodificación 45 de contenido. El procesador de mensajes 37 obtiene la clave privada (SEK_priv) del almacén 44 y utiliza ésta para extraer la TEK presente en el mensaje de STKM 15. Debido a que la clave privada (SEK_priv) obtenida del almacén 44 es la clave privada correspondiente a la clave pública (SEK_pub) utilizada para proteger la TEK, la TEK puede ser extraída por el procesador de mensajes 37 utilizando la correspondiente clave privada. El procesador de mensajes 37 a continuación pasa la TEK extraída al módulo de descodificación de contenido 45, el cual descodifica el contenido 13 codificado utilizando la TEK y permite que el contenido sea consumido – por ejemplo, que sea mostrado en la pantalla del terminal 1 de telefonía móvil y reproducido a través de los altavoces del terminal 1 de telefonía móvil.

Un segundo MNO 47 comparte la plataforma de emisión 7 y el generador de STKM 21 con el primer MNO 3. Cuando el generador de STKM 21 recibe una solicitud de STKM 19 desde la plataforma de emisión 7, la solicitud de STKM 19 permite que el generador de STKM 21 identifique para qué MNO ha sido solicitado un STKM y por lo tanto qué clave pública SEK se requiere. Por ejemplo, si la clave pública relevante no está presente en el almacén 23 y se requiere una SEK del segundo MNO 47, el generador de STKM 21 es operable para obtener del segundo MNO 47 una clave pública SEK enviando una solicitud de SEK al segundo MNO 47, de una manea similar al envío del mensaje de solicitud de SEK 25 al MNO 3. El segundo MNO 47 comprende un generador de STKM, el almacén de claves privadas y el generador de LTKM que operan en una manera similar al generador de SEK 17, el almacén de claves privadas 29 y el generador de LTKM 41 del MNO 3. El segundo MNO 47 establece las Claves de Usuario (UKs – User Keys, en inglés) para sus abonados y almacena éstas en los módulos seguros de sus abonados de una manera similar al primer MNO 3. El segundo MNO 47 también envía el LTKM 43, similar al LTKM 43 enviado por el primer MNO 3.

La plataforma de emisión 7 y el generador de STKM 21 pueden ser compartidos por los MNOs 3, 47 con poco riesgo de un compromiso de la seguridad porque sólo las claves públicas SEK de los MNOs 3, 47 son proporcionadas al generador de STKM 21 compartido (para una subsiguiente emisión por parte de la plataforma de emisión 7). Las correspondientes claves privadas SEK no son nunca proporcionadas al generador de STKM 21 compartido. Las claves privadas SEK son transmitidas mediante una comunicación de punto a punto en los LTKMs 43 por el MNO 3 (y el correspondiente LTKM para el MNO 47). Además, los LTKMs son protegidos utilizando la Clave de Usuario (UK – User Key, en inglés) relevante para una mayor mejora de la seguridad.

Aunque se muestran dos MNOs 3, 47 en la realización, debe comprenderse que la plataforma de emisión 7 y el generador de STKM 21 pueden ser compartidos por una multiplicidad de MNOs.

El esquema utilizado para emitir el contenido es DVB-H en la realización. No obstante, pueden utilizarse otros esquemas de emisión, tales como DVB-T, T-DMB, DAB-IP, ISDB-T, TDtv o Media FLO.

En la realización, el contenido es video (imágenes en movimiento y sonido). No obstante, debe comprenderse que el contenido podría ser de otros tipos – por ejemplo sólo sonido, imágenes quietas (presentación de imágenes), etc.

En la realización, el generador de STKM 21 y la plataforma de emisión 7 pueden ser una sola unidad.

El módulo seguro 5 puede ser implementado en hardware o software.

**REIVINDICACIONES**

1. Un método de controlar el uso, por parte de un terminal de usuario (1, $1^1$) registrado en una red de telecomunicaciones (3), de contenido (13) emitido mediante un medio de emisión (7) y codificado mediante una primera clave (TEK), incluyendo el método:

proporcionar la primera clave (TEK) al medio de emisión (7) para la emisión al terminal de usuario (1, $1^1$) con el contenido (13) codificado; y

caracterizado porque:

la red de telecomunicaciones (3) comparte un medio de codificación (21) con al menos otra red de telecomunicaciones (47);

la red de telecomunicaciones (3) genera una segunda clave pública (SEK_pub) y una correspondiente diferente pero relacionada tercera clave privada (SEK_priv);

la otra red de telecomunicaciones (47) genera una clave cuarta pública y una correspondiente diferente pero relacionada quinta clave privada;

el medio de codificación (21), es respuesta a una solicitud de un mensaje de clave (19), identifica para cuál de la red de telecomunicaciones (3) y la otra red de telecomunicaciones (47) se solicita el mensaje de clave (19) y, si el mensaje de clave (19) es solicitado para la red de telecomunicaciones (3), obtiene la segunda clave pública (SEK_pub) y codifica la primera clave (TEK) con la segunda clave pública (SEK_pub), o una clave derivada a partir de la segunda clave pública (SEK_pub), donde la primera clave codificada (33) es emitida por el medio de emisión (7) al terminal de usuario (1, $1^1$); y

proporcionar la tercera clave privada (SEK_priv) correspondiente a la segunda clave pública (SEK_pub) al terminal de usuario (1, $1^1$) mediante una comunicación de punto a punto entre la red de telecomunicaciones (3) y el terminal de usuario (1, $1^1$);

donde la tercera clave privada (SEK_priv) permite la extracción de la primera clave (TEK) para su uso en la descodificación del contenido (13).

2. El método de la reivindicación 1, en el que la comunicación de punto a punto entre la red de telecomunicaciones (3) y el terminal de usuario (1, $1^1$) envía la tercera clave privada (SEK_priv) codificada mediante otra clave.

3. El método de la reivindicación 1 ó 2, en el que el medio de emisión (7) es compartido por las redes de telecomunicaciones (3) y la otra red de telecomunicaciones (47).

4. El método de la reivindicación 1, 2 ó 3, en el que el medio de emisión (7) transmite la primera clave (TEK) al medio de codificación (21), y en el que el medio de codificación (21) transmite la primera clave codificada (33) al medio de emisión (7), para emisión directa al terminal de usuario (1, $1^1$).

5. El método de una cualquiera de las reivindicaciones 1 a 4, en el que el terminal de usuario (1, $1^1$) incluye un medio para recibir el contenido (13) codificado emitido y la primera clave (15) codificada emitida y para separar el contenido (13) codificado de la primera clave (15) codificada,

6. El método de una cualquiera de las reivindicaciones 1 a 5, en el que el terminal de usuario incluye una aplicación para acceder a la tercera clave privada (SEK_priv), para recibir la primer clave (15) codificada, y para derivar la primera clave (TEK) de la misma con el fin de permitir el consumo del contenido (13).

7. Un sistema para controlar el uso por parte de un terminal de usuario (1, $1^1$) de contenido (13) emitido mediante un medio de emisión (7) y codificado mediante una primera clave (TEK), incluyendo el aparato:

un medio (12) operable para proporcionar la primera clave (TEK) al medio de emisión para la emisión al terminal de usuario (1, $1^1$) con el contenido (13) codificado; y

caracterizado por:

una primera red de telecomunicaciones (3) operable para generar una segunda clave pública (SEK_pub) y una correspondiente diferente pero relacionada tercera clave privada (SEK_priv), estando el terminal de usuario (1, $1^1$) registrado en la primera red de telecomunicaciones (3);

al menos otra red de telecomunicaciones (47) operable para generar una cuarta clave pública y una correspondiente diferente pero relacionada quinta clave privada;

un medio de codificación (21) compartido por la primera red de telecomunicaciones (3) y la al menos otra red de telecomunicaciones (47), siendo el medio de codificación (21) operable, en respuesta a una solicitud de un mensaje de clave (19), para identificar para cuál de la red de telecomunicaciones (3) y la otra red de telecomunicaciones (47) se ha solicitado el mensaje de clave (19) y, si el mensaje de clave (19) se ha solicitado para la primera red de telecomunicaciones (3), obtener la segunda clave pública (SEK_pub) y codificar la primera clave (TEK) con la segunda clave pública (SEK_pub), o una clave derivada de la segunda clave pública (SEK_pub), donde la primera clave (13) codificada es emitida por el medio de emisión (7) al terminal de usuario (1, $1^1$); y

un medio operable para proporcionar la tercera clave privada (SEK_priv) correspondiente a la segunda clave pública (SEK_pub) al terminal de usuario (1, $1^1$) mediante comunicación de punto a punto entre la primera red de telecomunicaciones (3) y el terminal de usuario (1, $1^1$);

donde la tercera clave privada (SEK_priv) permite la extracción de la primera clave (TEK) para su uso en la descodificación del contenido (13).

8. El sistema de la reivindicación 7, en el que la comunicación de punto a punto entre la red de telecomunicaciones (3) y el terminal de usuario (1, $1^1$) envía la tercera clave privada (SEK_priv) codificada mediante otra clave.

9. El sistema de las reivindicaciones 7 u 8, en el que el medio de emisión (7) es compartido por las primeras redes de telecomunicaciones (3) y la otra red de telecomunicaciones (47).

10. El sistema de la reivindicación 7, 8 ó 9, en el que el medio de emisión (47) transmite la primera clave (TEK) al medio de codificación (21).

11. El sistema de una cualquiera de las reivindicaciones 7 a 10, en el que el terminal de usuario (1, $1^1$) incluye un medio para recibir el contenido (13) codificado emitido y la primera clave (15) codificada emitida, y para separar el contenido (13) codificado de la primera clave (15) codificada.

12. El sistema de una cualquiera de las reivindicaciones 7 a 11, en el que el terminal de usuario (1, $1^1$) incluye una aplicación para acceder a la tercera clave privada (SEK_priv) para recibir la primera clave (15) codificada, y para derivar la primera clave (TEK) de la misma para permitir el consumo del contenido (13).

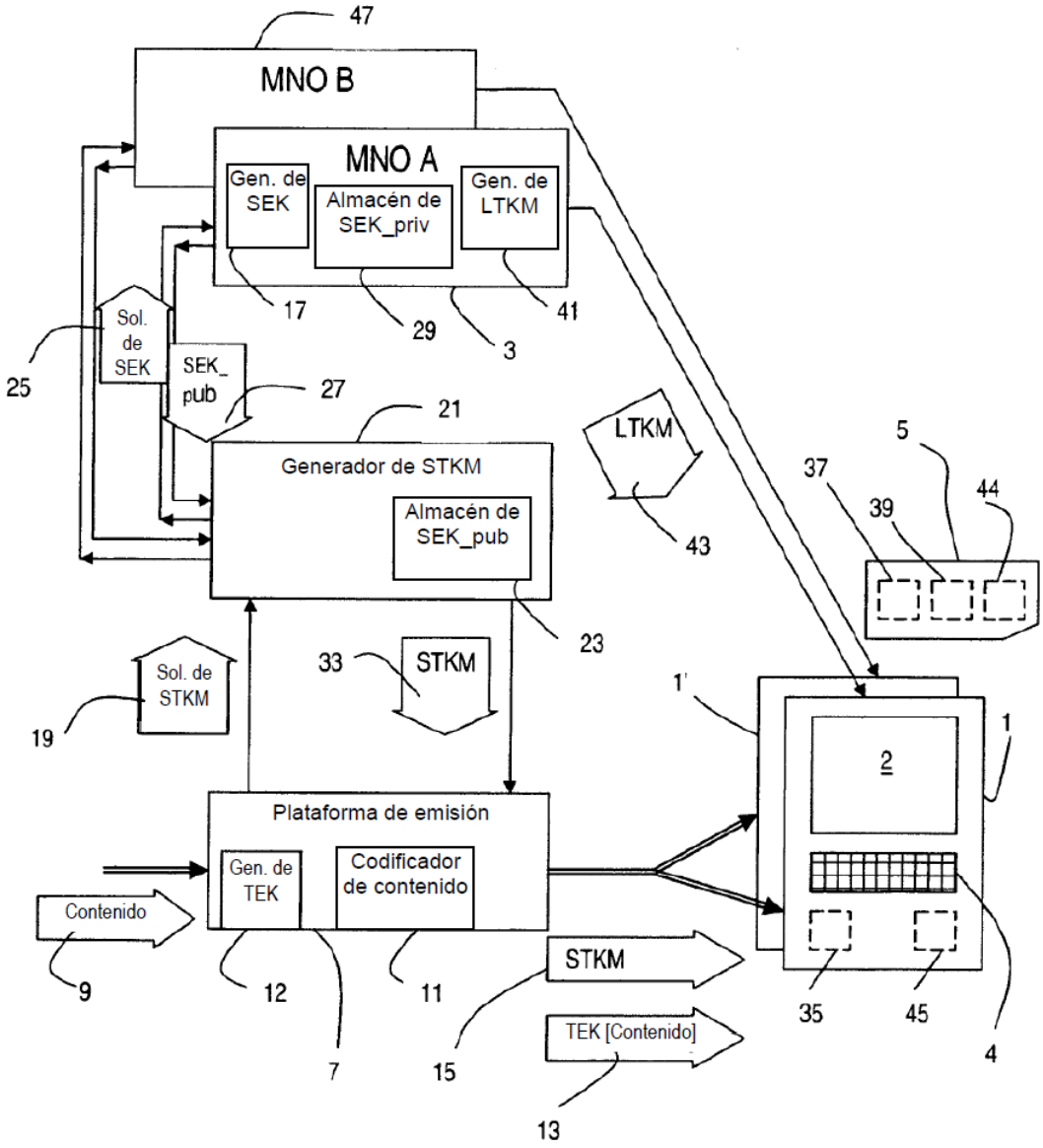
47
MNO B
MNO A
Gen. de SEK
Almacén de SEK_priv
Gen. de LTKM
17
29
41
3
Sol. de SEK
25
SEK_ pub
27
21
Generador de STKM
Almacén de SEK_pub
23
LTKM
43
5
37
39
44
Sol. de STKM
19
33
STKM
1'
1
2
Plataforma de emisión
Gen. de TEK
Codificador de contenido
Contenido
9
12
11
7
STKM
15
TEK [Contenido]
13
35
45
4

FIG. 1