(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 790 405**

(51) Int. CI.:

H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.11.2013 PCT/EP2013/074756**

(87) Fecha y número de publicación internacional: **30.05.2014 WO14080038**

(96) Fecha de presentación y número de la solicitud europea: **26.11.2013 E 13798309 (4)**

(97) Fecha y número de publicación de la concesión europea: **04.03.2020 EP 2923458**

(54) Título: **Método, sistema y dispositivo para transferir contenido de forma segura entre dispositivos dentro de una red**

(30) Prioridad:

26.11.2012 EP 12194223

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.10.2020

(73) Titular/es:

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

(72) Inventor/es:

BIEBER, YANN

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

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

DESCRIPCIÓN

Método, sistema y dispositivo para transferir contenido de forma segura entre dispositivos dentro de una red

Campo técnico

[0001] La presente invención se refiere al campo de la transferencia de contenido entre dispositivos dentro de una red gestionada por un centro de gestión, tal como un operador de dominio doméstico, que actúa como entidad de confianza para iniciar o activar comunicaciones entre dispositivos. Más específicamente, la invención pretende compartir contenido de forma segura entre un dispositivo de envío y al menos un dispositivo de recepción conectados entre sí dentro de una red por cable o inalámbrica después de haber realizado una fase de activación a través de un centro de gestión.

Estado de la técnica

[0002] Compartir contenido de forma segura entre dispositivos implica cifrar contenido con una o varias claves de cifrado, dependiendo del tipo de esquema criptográfico. El uso de una clave de encriptación/desencriptación compartida se refiere típicamente a un esquema de encriptación simétrico, mientras que el esquema asimétrico implica el uso de pares de claves privadas y públicas para cada dispositivo. La clave pública del dispositivo de recepción se puede intercambiar libremente a cualquier dispositivo y, por lo tanto, puede ser usada por un dispositivo de envío para encriptar un mensaje que se va a enviar al dispositivo de recepción. Este último usará su clave privada correspondiente para desencriptar el mensaje que no puede ser desencriptado por los otros dispositivos, dado que el proceso no es reversible, es decir, el mensaje encriptado no se puede desencriptar usando la clave pública del dispositivo de envío. Este esquema criptográfico se basa en un algoritmo que implica problemas matemáticos, que son fáciles de resolver de alguna manera, pero que son muy difíciles a la inversa. Como proceso de generación de clave compartida, el método Diffie-Hellman permite que dos partes establezcan conjuntamente una clave secreta compartida a través de un canal de comunicación inseguro y que posteriormente usen esta clave para encriptar comunicaciones posteriores según un esquema criptográfico simétrico.

[0003] En general, las claves se pueden asegurar perfectamente cuando se intercambian, fuera de los dispositivos, por medio de protocolos de red seguros y estas claves también se pueden asegurar perfectamente dentro de estos dispositivos, mediante rutas de clave de hardware. El problema ocurre cuando se conectan dos de estas partes, es decir, en la interfaz entre cada uno de estos dispositivos y las rutas de red que los conectan. Todas las comunicaciones entre dos dispositivos o sistemas requieren que los datos transferidos viajen hacia abajo a través de la pila de red del sistema de envío, a través de la capa física, y luego hacia arriba a través de la pila de red del sistema de recepción. La forma tradicional de conectar el protocolo de red seguro y la ruta de clave de hardware implica extraer la clave clara de la pila de red y luego introducirla en la ruta de clave de hardware. Esta manera de hacerlo expone la clave clara usada para realizar operaciones criptográficas en el contenido de la memoria RAM del dispositivo. Por lo tanto, existe el riesgo de que una persona malintencionada que quiera interceptar los mensajes intercambiados entre dos dispositivos pueda acceder a esta clave dentro del dispositivo antes de introducirla en la ruta de clave de hardware. Por consiguiente, transferir un contenido seguro entre dispositivos implica el uso de al menos una clave criptográfica que se debe intercambiar de forma segura entre los mismos dispositivos para evitar cualquier piratería por parte de personas malintencionadas.

[0004] El documento US 2010/250933 A1 divulga un método para una red entre pares donde el contenido almacenado dentro de un dispositivo de red se registra en un servidor de gestión de contenido y una clave de contenido es generada por un servidor de entrega de clave. La clave de contenido se encripta para cada dispositivo de red con su clave de dispositivo y luego se transfiere al dispositivo respectivo. El contenido se encripta usando la clave de contenido y se carga desde el(los) dispositivo(s) de red de origen y se descarga a un dispositivo de red objetivo.

[0005] El documento US 6,363,154 B1 divulga un método para enviar mensajes seguros desde un miembro de grupo a una pluralidad de miembros de grupo dentro de un grupo. En primer lugar, una clave de grupo (también denominada clave secreta aleatoria) es establecida por un miembro. Posteriormente, esta clave de grupo es distribuida por este miembro a los otros miembros del grupo. Cuando un miembro del grupo quiere distribuir un mensaje a una pluralidad de miembros de grupo, este miembro puede generar una clave de trabajo según un proceso de derivación de clave. Para este fin, este miembro genera un número aleatorio y realiza una función control, aplicada tanto en el número aleatorio como en la clave de grupo, para obtener la clave de trabajo. El mensaje se encripta usando la clave de trabajo antes de enviar tanto el mensaje encriptado como el número aleatorio a los otros miembros de grupo. Estos últimos deben llevar a cabo la misma función control usando la clave de grupo y el número aleatorio adjunto al mensaje encriptado para obtener la clave de trabajo requerida para desencriptar el mensaje. En otra forma de realización, el mensaje se puede encriptar con una denominada "clave de encriptación de datos" que se transmite junto con el mensaje anteriormente mencionado en una forma encriptada usando la clave de trabajo.

[0006] El documento WO 2006/089101 A2 divulga un método para autenticar un dispositivo cliente con un servidor de autenticación usando un código de autenticación. El dispositivo cliente se identifica mediante un identificador exclusivo. Inicialmente, un generador de semillas genera y envía una semilla maestra tanto a un servidor de claves como a un token de hardware usados para generar el código de autenticación para el dispositivo cliente. La semilla maestra puede considerarse como un secreto que solo es compartido por el token y por el servidor de claves. Gracias a una función de derivación de claves, tanto el servidor de claves como el token pueden generar una semilla derivada, que es específica para cada dispositivo cliente. La semilla derivada combina matemáticamente la semilla maestra y el identificador exclusivo del dispositivo cliente. El token de hardware se conecta al dispositivo cliente y el servidor de autenticación se conecta al servidor de claves. Por consiguiente, la semilla derivada puede ser usada por el token de hardware para producir el código de autenticación. Este código de autenticación es transmitido por el token de hardware al dispositivo cliente, que lo reenvía al servidor de autentificación. Por su parte, el servidor de autenticación puede obtener la misma semilla derivada del servidor de claves. Por consiguiente, el servidor de autenticación puede generar el código de autenticación y puede compararlo con el recibido desde el dispositivo cliente. Si hay una coincidencia, el código de autenticación se valida.

Resumen de la invención

[0007] La invención es definida por las reivindicaciones anexas. Para resolver el problema anteriormente mencionado, la presente invención pretende sugerir un método para transferir contenido de forma segura entre dispositivos dentro de una red. Por ejemplo, dicha red puede ser gestionada por un centro de gestión. Los dispositivos pueden ser de diferentes tipos. Por ejemplo, pueden referirse a medios de almacenamiento y comunicación, decodificadores, puertas de enlace, sistemas de televisión o cualquier otro dispositivo capaz de intercambiar datos dentro de una red. Dicha red puede ser una red local (por ejemplo, un dominio doméstico), una red amplia, como Internet, o cualquier otro especie de red adecuada para conectar dispositivos de comunicación. Cada dispositivo de la red se precarga con un valor secreto exclusivo preinicializado previamente almacenado en una memoria segura de un chip dentro del dispositivo. Esto normalmente se logra durante la fabricación de los chips, que luego se implementan en los dispositivos. La asignación de un valor secreto a cada conjunto de chips se realiza generalmente por parte de una autoridad de personalización para que nadie más conozca este valor secreto. Este valor secreto preinicializado es diferente para cada dispositivo.

[0008] El centro de gestión se usa para iniciar las comunicaciones de dispositivos a través de la red al proporcionarles datos de activación que luego son usados por estos dispositivos para comunicarse entre sí. Para este fin, el centro de gestión tiene, para cada uno de los dispositivos de la red, una clave de dispositivo K y un valor de dispositivo V, que son datos personales que pertenecen a cada dispositivo (es decir, exclusivos y diferentes para cada dispositivo). Estos datos personales han sido previamente transmitidos al centro de gestión por la autoridad de personalización. El valor de dispositivo V es el resultado de una operación criptográfica preliminar realizada en la clave de dispositivo K por medio del valor secreto S correspondiente al mismo dispositivo.

[0009] El método comprende, en primer lugar, una fase de activación (es decir, una fase de inicialización) para activar todos los dispositivos de la red que quieren enviar o intercambiar mutuamente contenido CT. Esta fase de activación comprende los pasos de:

- generar, por el centro de gestión, una clave de red KN común a todos los dispositivos anteriormente mencionados,
- calcular, por el centro de gestión y para cada uno de dichos dispositivos, una clave de red encriptada KN', que es el resultado de la encriptación de la clave de red KN por medio de la clave de dispositivo K correspondiente,
- transmitir, por el centro de gestión a cada uno de dichos dispositivos, su valor de dispositivo V y su clave de red encriptada KN'.

[0010] En segundo lugar, el método comprende una fase de recuperación de claves, que es realizada por cada uno de los dispositivos que quieren comunicarse entre sí. Dicha fase de recuperación de claves comprende los siguientes dos pasos:

- realizar una primera operación criptográfica para obtener la clave de dispositivo K a partir del valor de dispositivo V recibido y a partir del valor secreto S de dicho dispositivo,
- realizar una segunda operación criptográfica para obtener la clave de red KN a partir de la clave de red encriptada recibida KN' y a partir de la clave de dispositivo K.

[0011] Finalmente, el método comprende una fase operativa realizada por cada dispositivo involucrado en la transferencia de contenido CT y datos asociados. Por consiguiente, tal fase de transferencia incluye encriptar y

enviar datos desde el dispositivo de envío y recibir y desencriptar dichos datos mediante al menos un dispositivo de recepción. Esta fase operativa comprende los pasos de:

- generar un valor aleatorio RV, o extraer dicho valor aleatorio RV de los datos asociados anteriormente mencionados durante una tercera operación criptográfica, con el objetivo de usar posteriormente dicho valor aleatorio RV, respectivamente, para la encriptación o la desencriptación de dicho contenido CT,

- generar una clave final al encriptar el valor aleatorio RV por medio de la clave de red KN o al usar dicho valor aleatorio RV como clave final, directa o indirectamente, como lo proporciona dicha tercera operación criptográfica,

- usar la clave final para encriptar o desencriptar dicho contenido CT.

[0012] Las operaciones de encriptación o desencriptación anteriormente mencionadas, mencionadas en esta fase operativa, dependen de si se refieren al dispositivo de envío o al dispositivo de recepción respectivamente.

[0013] Según un aspecto más general, el paso destinado a generar la clave final podría ser llevado a cabo

- realizando una operación criptográfica que involucra el valor aleatorio RV y la clave de red KN, o

- usando dicho valor aleatorio RV como clave final, directa o indirectamente, como lo proporciona dicha tercera operación criptográfica.

[0014] Según una segunda formulación, la fase operativa también podría comprender los siguientes pasos:

- generar un valor aleatorio RV en uno de dichos dispositivos que actúa como dispositivo de envío,

- realizar, en el dispositivo de envío, una tercera operación criptográfica para generar una clave de contenido Kc a partir de dicho valor aleatorio RV y a partir de la clave de red KN,

- encriptar el contenido CT con dicha clave de contenido Kc o con dicho valor aleatorio RV y, respectivamente,

- enviar el contenido encriptado CT' con el valor aleatorio RV o con la clave de contenido Kc como datos asociados a al menos uno de dichos dispositivos que actúa como dispositivo de recepción.

[0015] En otras palabras, los dos últimos pasos de esta segunda formulación también podrían ser mencionados por dos alternativas de la siguiente manera:

- encriptar el contenido CT con dicha clave de contenido Kc, luego enviar el contenido encriptado CT' y el valor aleatorio RV a al menos uno de dichos dispositivos que actúan como dispositivo de recepción,
  o

- encriptar el contenido CT con dicho valor aleatorio RV, luego enviar el contenido encriptado CT' y la clave de contenido Kc a al menos uno de dichos dispositivos que actúan como dispositivo de recepción.

[0016] Según la segunda formulación anteriormente mencionada, el método comprende además los pasos de:

- realizar, en el dispositivo de recepción, la misma tercera operación criptográfica para generar la clave de contenido Kc a partir del valor aleatorio recibido RV y a partir de la clave de red KN,

- desencriptar, en el dispositivo de recepción, el contenido encriptado CT' por medio de la clave de contenido Kc.

[0017] Según una forma de realización preferida de la presente invención, el valor de dispositivo V, asignado a cada dispositivo, se almacena al recibirlo en una memoria segura del dispositivo. Ventajosamente, esta memoria segura se encuentra dentro de un chip monolítico que realiza todas las operaciones criptográficas en el dispositivo. De este modo, la encriptación/desencriptación del contenido y las operaciones criptográficas primera, segunda y tercera se realizan dentro de un único chip, es decir, un chip monolítico, en cada dispositivo.

[0018] Una de las ventajas principales del presente método es que cualquier dato que se introduce en este chip (o sale de este chip) no es suficiente para desencriptar un contenido encriptado por este chip. Cabe señalar que los datos asociados (es decir, el valor aleatorio RV o la clave de contenido Kc asociados al contenido encriptado) no se pueden usar sin realizar una operación criptográfica en dichos datos asociados por medio de la clave de red KN (tercera operación criptográfica). Además, debe tenerse en cuenta que dicha clave de red KN requiere dos

operaciones criptográficas sucesivas (operaciones criptográficas primera y segunda) que solo se realizan dentro de los dispositivos, en particular, dentro del chip de cada uno de estos dispositivos. Por lo tanto, cualquier piratería de las comunicaciones que entran y salen de este chip no permite que una persona malintencionada descodifique los contenidos encriptados por un dispositivo de envío conforme al presente método. De hecho, y según una segunda ventaja principal de la presente invención, la clave final que protege el contenido nunca aparece de manera clara, ni en la RAM de uno de los dispositivos, ni a través de la red.

[0019] Asimismo, el presente método permite encriptar/desencriptar el contenido con una única clave final, es decir, conforme a un esquema de encriptación/desencriptación simétrico. Por consiguiente, este método proporciona un proceso criptográfico rápido y eficiente que ahorra tiempo y recursos informáticos a todos los dispositivos de la red.

[0020] Ventajosamente, el contenido y los datos criptográficos ("material" criptográfico, es decir, los denominados "datos asociados") intercambiados entre los dispositivos de la red no transitan a través del centro de gestión, sino que se envían directamente desde el dispositivo de envío a los receptores. Por consiguiente, el centro de gestión ya no es útil una vez que los dispositivos han realizado la fase de activación. Esta es otra ventaja principal de la presente invención, dado que la fase operativa que pretende transferir datos de forma segura (incluido el contenido CT) entre los dispositivos conectados a la red puede ser llevada a cabo por cualquier dispositivo sin requerir intercambios de datos adicionales con el centro de gestión. En consecuencia, la transferencia de datos es más rápida y el centro de gestión se puede liberar para realizar otras tareas. Otras ventajas y formas de realización se presentarán en la siguiente descripción detallada.

[0021] La presente invención también sugiere un sistema para transferir contenido de forma segura entre dispositivos dentro de dicha red. Además, la presente invención también se refiere a un dispositivo para transferir contenido de forma segura con otros dispositivos idénticos dentro de esta red.

Breve descripción de los dibujos

[0022] La presente invención se entenderá mejor gracias a las figuras adjuntas en las que:

La figura 1 es un diagrama de bloques que muestra los operadores principales del método de la presente invención y las operaciones principales realizadas dentro de cada uno de estos para iniciar la transmisión de datos y para intercambiar datos de forma segura (es decir, contenido y datos asociados) entre los dispositivos de la red,

La figura 2 se refiere a una variante de la figura 1, que representa solo las diferencias con respecto a la figura 1, de modo que los elementos que no difieren de la figura 1 no se han mostrado en aras de la simplificación.

Descripción detallada

[0023] Ahora se hará referencia en detalle a la forma de realización preferida de la invención, como se ilustra en la figura 1. En aras de la simplificación, solo se han mostrado dos dispositivos en esta figura, sin embargo, se entenderá que el método de la presente invención obviamente no se limita a dos dispositivos, sino que puede involucrar muchos dispositivos.

[0024] Esta figura muestra, en primer lugar, un centro de gestión 1 y dos dispositivos 10, 20, que están destinados a intercambiar un contenido CT entre ellos, en particular a enviar y recibir dicho contenido CT. En este ejemplo, el primer dispositivo actúa como dispositivo de envío 10 y el segundo actúa como dispositivo de recepción 20. Los dos dispositivos 10, 20 están conectados entre sí por medio de una red ilustrada por flechas dibujadas entre ellos. El centro de gestión 1 puede ser parte de esta red o se puede conectar a los dispositivos a través de otra red. Preferiblemente, la misma red, por ejemplo internet, permite la interconexión tanto del centro de gestión 1 como de los dispositivos 10, 20 involucrados en el método de la invención. Sin embargo, otros soportes, tales como una red telefónica o cualquier otro medio de soporte, podrían ser usados por el centro de gestión 1 para proporcionar datos de activación a cada uno de los dispositivos 10, 20.

[0025] Durante la fabricación o la personalización de chips situados en los dispositivos, una autoridad de personalización 30 ha almacenado un valor secreto S en la memoria de cada uno de estos chips, en particular en una memoria segura no volátil. Este valor secreto es exclusivo para cada dispositivo y se identifica respectivamente mediante S1, S2 en la figura 1 y esta operación se muestra mediante las líneas de puntos y discontinuas en esta figura. Como esta operación se realiza durante la fabricación o durante la personalización del chip por parte de una autoridad de confianza, el valor secreto S asignado a cada dispositivo se puede considerar como implementado de una manera totalmente secreta y segura. De una manera similar, la clave de dispositivo K y el valor de dispositivo V, que pertenecen a a cada dispositivo 10, 20, están determinados por la autoridad de personalización e se implementan en la memoria del centro de gestión durante su uso. Esta operación se muestra en la figura 1 con las líneas discontinuas. El valor de dispositivo V asignado a cada dispositivo es el resultado de una operación criptográfica preliminar de la clave de dispositivo K por medio del valor secreto S. Este se muestra

en esta figura mediante las expresiones $V_1=(K_1)_{S1}$; $V_2=(K_2)_{S2}$ observadas en el módulo criptográfico preliminar 38 de la autoridad de personalización que es responsable de determinar el valor de dispositivo V, la clave de dispositivo K y el valor secreto S para cada dispositivo. Cada clave de dispositivo K y cada valor de dispositivo V que pertenecen al mismo dispositivo también pueden almacenarse en el registro asignado a este dispositivo y almacenarse en la memoria 36 de la autoridad de personalización 30.

[0026] A partir de esta configuración, el método comprende, en primer lugar, una fase de activación durante la cual el centro de gestión interactúa con los dispositivos, en particular con los nuevos dispositivos que forman o se unen a la red, con la finalidad de enviar o intercambiar datos mutuamente (incluido el contenido CT). Entonces, este método se refiere a una fase de recuperación de claves y a una fase operativa durante la cual los contenidos CT (es decir, datos o mensajes) se intercambian entre dispositivos específicos sin ninguna interacción desde el centro de gestión.

[0027] El centro de gestión 1 comprende una memoria 6, que almacena, para cada dispositivo 10, 20 de la red, al menos una clave de dispositivo K y un valor V. Como se muestra en esta figura, la clave de dispositivo K_1 y el valor de dispositivo V_1 pertenecen al primer dispositivo 10, mientras que la segunda clave de dispositivo K_2 y el segundo valor de dispositivo V_2 se reservan para el segundo dispositivo 20. Por lo tanto, en una red que comprende n dispositivos, la memoria 6 almacena las claves de dispositivo K_1, K_2, ..., K_n y los valores de dispositivo V_1, V_2, ..., V_n. En la presente descripción y en aras de la claridad, el número de índice 1, 2, ..., n asociado a las letras alfabéticas siempre se refiere al dispositivo designado por el mismo índice (por lo tanto, el número de índice 1 se refiere al primer dispositivo, el número de índice 2 se refiere al segundo dispositivo, etc).

[0028] Durante la inicialización de la red, es decir, durante la activación de sus dispositivos, el centro de gestión 1 genera una clave de red KN por medio de un generador de clave 4. La clave de red KN es una clave común que será usada por todos los dispositivos y que preferiblemente se genera de forma aleatoria. Sin embargo, esta clave de red nunca se transmite en texto sencillo a través de la red. Dentro del centro de gestión, la clave de red KN se introduce en un módulo de encriptación 5 para calcular, para cada dispositivo 10, 20, una clave de red encriptada KN'.

[0029] La clave de red encriptada KN' está determinada por el algoritmo del módulo de encriptación 5, que requiere, como entrada adicional, la clave de dispositivo K. Por ejemplo, la clave encriptada KN'_1, que se refiere al primer dispositivo 10, se calcula encriptando la clave de red común KN por medio de la clave de dispositivo K_1 asignada al primer dispositivo. El módulo de encriptación 5 puede usar cualquier tipo de algoritmo para generar las claves de red encriptadas KN'_n. Como se muestra en la figura 1, el centro de gestión también tiene valores de dispositivo V almacenados en su memoria 6. Por ejemplo, la clave de dispositivo K_1 y el valor de dispositivo V_1 se pueden almacenar conjuntamente en un único registro asignado al primer dispositivo 10. Alternativamente, se pueden almacenar por separado si son identificados, por ejemplo, por un índice n usado para designar el mismo dispositivo exclusivo. En cualquier caso, la clave de dispositivo K y el valor de dispositivo V se refieren a datos personales que son preferiblemente exclusivos para cada dispositivo.

[0030] La clave de red KN' y el valor de dispositivo V correspondiente corresponden a los denominados datos de activación. Cada clave de red encriptada KN' y cada valor de dispositivo V se transmiten posteriormente desde el centro de gestión al dispositivo 10, 20 correspondiente, preferiblemente por medio de una unidad de envío 7 a través de una interfaz adecuada. Se podrían usar otros medios de transmisión. Además, la clave de red encriptada KN'_1 y el valor de dispositivo V_1 se pueden enviar conjuntamente en un único mensaje de activación (paquete o registro) al dispositivo 10, o se pueden enviar por separado sin un orden específico. Las direcciones electrónicas usadas para enviar estos datos a los dispositivos apropiados pueden ser gestionadas por el propio centro de gestión o por una tercera unidad dentro de la red. Como se muestra en la figura 1, los componentes 4, 5, 6, y 7 pertenecen al centro de gestión 1.

[0031] Ahora con referencia más específica al dispositivo 10, este último actúa como dispositivo de envío y tiene que enviar de forma segura el contenido CT al segundo dispositivo 20, como se representa en el ejemplo de la figura 1. Para este fin, el dispositivo de envío 10 necesita varios componentes, en particular un primer módulo criptográfico 11, un segundo módulo criptográfico 12, un tercer módulo criptográfico 13, un generador de valor aleatorio 14, un módulo criptográfico de contenido 15 y una memoria 16. Todos estos componentes, excepto el generador de valor aleatorio 14, se incluyen en un único chip 18. Alternativamente, el generador de valor aleatorio 14 también podría situarse dentro del chip 18. Este chip 18 está provisto de una interfaz de comunicación, que permite recibir datos, en particular al menos el valor de dispositivo V y la clave de red encriptada KN', preferiblemente también un valor aleatorio RV generado por el generador 14 (en el caso de que este último se encuentre fuera del chip 18). Esta interfaz de comunicación también se puede usar para enviar el contenido, una vez que se ha encriptado, a al menos un receptor. Esta interfaz se usa además para enviar datos asociados, tales como un valor aleatorio, por ejemplo en el caso de que el generador de valor aleatorio 14 se encuentre dentro del chip 18. Como se muestra en la figura 1, cada dispositivo 10, 20 de la red puede comprender ventajosamente los mismos componentes que los descritos con referencia al primer dispositivo 10.

[0032] Según una forma de realización preferida, el valor de dispositivo V y la clave de red encriptada KN' (recibidos, por ejemplo, dentro de un mensaje de activación) se almacenan dentro de una memoria no volátil 17 asociada al dispositivo 10 para su uso posterior. Como se muestra en la figura 1, tal memoria no volátil 17 no es necesariamente una memoria segura y, por lo tanto, podría situarse fuera del chip 18, por ejemplo dentro del dispositivo 10. Sin embargo, es ventajoso colocar la memoria no volátil 17 dentro del chip 18, de modo que pueda ser protegida por el conjunto de chips. Una vez que los datos de activación (V, KN') han sido recibidos por el dispositivo 10, 20, la fase de activación finaliza y la siguiente fase se refiere a una fase de recuperación de claves (destinada a recuperar sucesivamente la clave de dispositivo K y la clave de red KN, como se describe a continuación).

[0033] Al recibir el dispositivo 10, el valor de dispositivo V también se puede introducir directamente en el primer módulo criptográfico 11, junto con el valor secreto S recuperado de esta memoria 16. Debido a su algoritmo y a estas dos entradas V, S, el primer módulo criptográfico 11 puede deducir la clave de dispositivo K, que pertenece al dispositivo de envío 10. De hecho, dado que el valor de dispositivo V es el resultado de la operación criptográfica preliminar de la clave de dispositivo K por medio del valor secreto S, es decir $V=(K)_S$, por lo tanto, al usar un algoritmo inverso en el primer módulo criptográfico 11, la clave de dispositivo K se puede determinar a partir del valor de dispositivo V y del valor secreto S. Entonces, la clave de red encriptada KN' se introduce junto con la clave de dispositivo K en el segundo módulo criptográfico 12, que realiza la operación criptográfica inversa a la realizada por el módulo de encriptación 5 del centro de gestión 1. Por consiguiente, la clave de red KN se puede recuperar. La clave de red KN preferiblemente no se memoriza dentro del chip de los dispositivos (por ejemplo, en una memoria segura), pero se determina siempre que sea necesario en base a los datos de activación (V, KN') que se memorizan preferiblemente dentro de cada dispositivo, una vez recibidos del centro de gestión.

[0034] Una vez que la clave de red KN es determinada y conocida por el dispositivo 10, la fase de recuperación de claves finaliza. La clave de red KN, que es común a todos los dispositivos 10, 20 de la red, puede ser determinada, de la misma manera, por cada uno de ellos y se puede usar muchas veces sin requerir ningún cambio. Esto significa que se han realizado los mismos pasos de activación y de recuperación de claves con el(los) otro(s) dispositivo(s) 20, de modo que, ventajosamente, todos los dispositivos 10, 20 de la red tienen la misma clave de red KN.

[0035] En una variante, la clave de red KN podría ser almacenada en una memoria segura dentro del chip del dispositivo para su uso posterior. Sin embargo, según la forma de realización preferida, la clave de red KN nunca se almacena y, por lo tanto, debe determinarse por medio de los datos de activación (V, KN') siempre que sea necesario, es decir, cada vez que se deba procesar un contenido CT, CT'. Esto se puede hacer fácilmente si los datos de activación se han memorizado en la memoria no volátil 17 al recibirlos desde el centro de gestión.

[0036] Los siguientes pasos se refieren a la fase operativa (o fase de transferencia) durante la cual se realiza y procesa la transferencia de datos, incluido el contenido CT y los datos asociados. Por consiguiente, la fase operativa pretende preparar los datos que se van a transferir de forma segura, luego enviar datos y recibir y procesar tales datos en el receptor.

[0037] Para este fin, el dispositivo de envío 10 genera, por medio de su generador de valor aleatorio 14, un valor aleatorio RV, que se introduce en el tercer módulo criptográfico 13, con la clave de red KN. Debido al algoritmo implementado en el tercer módulo criptográfico, se determina una clave de contenido Kc, como clave final, a partir de las dos entradas RV y KN, preferiblemente usando la clave de red KN como clave para encriptar el valor aleatorio RV. El último módulo del chip 18 es el módulo criptográfico de contenido 15, que encripta un contenido CT por medio de la clave final, es decir, la clave de contenido Kc en esta forma de realización. Evidentemente, la encriptación se lleva a cabo por medio del algoritmo de encriptación implementado en el módulo criptográfico de contenido 15. A la salida de este último módulo, el contenido encriptado CT' se transmite posteriormente al receptor apropiado por medio de un proceso de enrutamiento común (por ejemplo, que involucra la dirección electrónica del dispositivo de recepción 20). El valor aleatorio RV proporcionado por el generador de valor aleatorio 14 también se envía a este receptor 20 como datos asociados, ya sea separado del contenido encriptado CT', o conjuntamente dentro de un mensaje común. El chip 18, y/o el dispositivo 10 pueden usar la misma interfaz de comunicación para recibir y enviar datos.

[0038] Según una variante, denominada "variante de transferencia CT", el módulo criptográfico de contenido 15 podría encriptar el contenido CT, por medio del valor aleatorio RV, como clave final (en vez de usar la clave de contenido Kc). Entonces, en vez de enviar al receptor 20 el valor aleatorio RV como datos asociados al contenido encriptado CT', el dispositivo de envío 10 envía al receptor 20 la clave de contenido Kc como datos asociados. Este caso se muestra en la parte de izquierda de la figura 2, que representa dicha "variante de transferencia CT", en particular solo lo que es diferente con respecto a la solución preferida ilustrada en la figura 1. Preferiblemente, la clave de contenido Kc corresponde a la encriptación del valor aleatorio RV por medio de la clave de red KN.

[0039] Volviendo a la figura 1, la fase operativa descrita anteriormente también puede comprender los pasos de recibir el contenido encriptado CT' y el valor aleatorio RV mediante el dispositivo de recepción 20, más particularmente mediante el único chip 28 de este dispositivo. El valor aleatorio RV se introduce, con la clave de

red KN determinada por el dispositivo de recepción 20, en el tercer módulo criptográfico 23 de este segundo dispositivo. Este módulo realiza la misma operación criptográfica que que la llevada a cabo por el tercer módulo criptográfico 13 del primer dispositivo 10. Por consiguiente, el dispositivo de recepción 20 es capaz de generar la misma clave de contenido Kc que la del primer dispositivo, dado que la clave de red KN es idéntica para todos los dispositivos, como se mencionó anteriormente. Al usar su propio módulo criptográfico de contenido 25, provisto del mismo algoritmo reversible de encriptación/desencriptación que el implementado en el módulo 15 del dispositivo de envío 10, el dispositivo de recepción 20 finalmente puede desencriptar el contenido encriptado CT' por medio de la clave de contenido Kc, como se muestra en la figura 1.

[0040] Como alternativa y de acuerdo con la "variante de transferencia CT" anteriormente mencionada, mostrada en la figura 2 (en particular ahora con la parte derecha de esta figura), la fase operativa también puede comprender los pasos de recibir el contenido encriptado CT' y la clave de contenido Kc (es decir, los datos asociados) mediante el dispositivo de recepción 20, más particularmente mediante el único chip 28 de este dispositivo. La clave de contenido Kc se introduce, con la clave de red KN, determinada por el dispositivo de recepción 20, en el tercer módulo criptográfico 23 de este segundo dispositivo. Este módulo realiza una operación criptográfica similar a la llevada a cabo por el tercer módulo criptográfico 13 del primer dispositivo 10. Por consiguiente, el dispositivo de recepción 20 es capaz de generar el mismo valor aleatorio RV que el del primer dispositivo, dado que la clave de red KN es idéntica para todos los dispositivos. Al usar su propio módulo criptográfico de contenido 25, provisto del mismo algoritmo reversible de encriptación/desencriptación, que el implementado en el módulo 15 del dispositivo de envío 10, el dispositivo de recepción 20 es finalmente capaz de desencriptar el contenido encriptado CT' por medio del valor aleatorio RV (que actúa como clave final).

[0041] De acuerdo con la denominada "variante de transferencia CT", mostrada en la figura 2, cabe señalar que los dos módulos criptográficos terceros 13 y 23 implican los mismos valores, es decir, KN, RV y Kc. Según el módulo criptográfico 13, el valor de entrada es RV y este módulo permite obtener Kc (como datos asociados) por medio de la clave KN, mientras que, según el módulo criptográfico 23, el valor de entrada es Kc (es decir, dichos datos asociados) y permite obtener RV (como clave final) por medio de la misma clave KN.

[0042] Para generalizar las dos posibles formas (es decir, la primera forma descrita y su denominada "variante de transferencia CT"), se puede mencionar que la fase operativa también puede comprender los pasos de:

- obtener una clave de desencriptación final al realizar, en el dispositivo de recepción, la misma o una tercera operación criptográfica 23 similar, que involucra la clave de red KN, el valor aleatorio RV y la clave de contenido Kc, luego
- desencriptar, en el dispositivo de recepción, el contenido encriptado CT' por medio de la clave final (clave de desencriptación).

[0043] Dependiente de los datos, es decir, Kc o RV, elegidos para encriptar el contenido CT en el contenido encriptado CT', la clave final anteriormente mencionada para desencriptar el contenido encriptado CT' puede ser respectivamente la clave de contenido Kc o el valor aleatorio RV.

[0044] En otras palabras, y con el fin de generalizar la fase operativa, sea cual sea la forma de realización y/o el dispositivo (es decir, el dispositivo de envío o el dispositivo de recepción), se puede resumir que esta fase comprende los siguientes pasos:

- generar, o extraer, a partir de los datos asociados anteriormente mencionados durante una tercera operación criptográfica, un valor aleatorio RV que se usará posteriormente, de manera respectiva, para la encriptación o la desencriptación del contenido CT,

- generar una clave final al encriptar el valor aleatorio RV por medio de la clave de red KN o al usar dicho valor aleatorio RV como clave final, directa o indirectamente, como lo proporciona la tercera operación criptográfica,

- usar dicha clave final para encriptar o desencriptar dicho contenido CT.

[0045] Como se muestra en la figura 1, y según otra forma de realización, el valor aleatorio RV se puede almacenar en la memoria no volátil 27 una vez recibido por el dispositivo de recepción 20. Si es necesario, por ejemplo en el caso de que los datos de activación pudieran cambiar, el valor de dispositivo V y la clave de red encriptada KN' también se guardan, por ejemplo, en la memoria no volátil, ya sea en el dispositivo de recepción 20, o en el dispositivo de envío o en ambos dispositivos. Según una forma de realización, la clave final podría almacenarse en una memoria no volátil segura del dispositivo. En el caso de que el contenido encriptado CT' se refiera a datos importantes, podría ser apropiado guardarlo junto con el valor aleatorio RV, también preferiblemente con los datos de activación V, KN' correspondientes, en al menos dos dispositivos 10, 20.

[0046] Preferiblemente, los módulos criptográficos primero, segundo y tercero 11, 12, 13 y 21, 22, 23 del mismo chip 18, 28 usan algoritmos diferentes entre sí. Sin embargo, el mismo algoritmo se puede usar en varios módulos criptográficos del mismo chip. No obstante, es necesario que los terceros módulos criptográficos 13, 23 de los respectivos chips 18, 28 usen el mismo algoritmo criptográfico para asegurar una correcta encriptación/desencriptación mutua del contenido. De forma similar, el primer módulo criptográfico y el segundo criptográfico (de cualquier chip) deben usar el(los) mismo(s) algoritmo(s) criptográfico(s) que el(los) usado(s) respectivamente por el módulo criptográfico preliminar 38 y por el módulo de encriptación 5.

[0047] Este es el final de la fase operativa, que se puede repetir cada vez que un contenido CT deba ser enviado desde un dispositivo a al menos un otro dispositivo dentro de la misma red (es decir, un dispositivo podría enviar el mismo contenido encriptado CT, junto con el mismo valor aleatorio RV, a una pluralidad de dispositivos activados). El mismo contenido encriptado CT' y el valor aleatorio encriptado RV' correspondiente se pueden compartir a cualquier dispositivo de la red doméstica que realizó la misma fase de activación.

[0048] Además, y según una forma de realización particular, también podría ser posible que el dispositivo 10 actúe como dispositivo de envío y como dispositivo de recepción al enviarse a sí mismo un contenido encriptado CT'. Dicho modo podría usarse para almacenar localmente un contenido encriptado CT' (en el presente ejemplo dentro del dispositivo 1), mientras se sabe que este contenido encriptado se puede desencriptar en el futuro para su uso posterior. Para este fin, el contenido encriptado CT' y los datos asociados, es decir, el valor aleatorio RV relevante (o la clave de contenido Kc de acuerdo con la "variante de transferencia CT") se pueden almacenar en cualquier memoria dentro del entorno del dispositivo 10, por ejemplo, en una memoria ubicada fuera del chip 18, como la memoria no volátil 17, o en un medio de almacenamiento externo (por ejemplo, CD, DVD, medio de almacenamiento USB) conectable al dispositivo 10. Si cualquier dato de activación V_1, KN'_1 está sujeto a ser cambiado antes de que el contenido encriptado CT' se desencripte, los datos de activación también se almacenarán en esta memoria no volátil 17 (o en dichos medios de almacenamientos externos). En una variante, en vez de almacenar los datos de activación V_1 y KN'_1, la clave de red KN se podría almacenar en una memoria segura dentro del chip 18. En cualquier caso, el dispositivo 10 tiene, en cualquier momento, todos los datos requeridos para recuperar la clave de contenido Kc con el objetivo de desencriptar el contenido encriptado CT' almacenado.

[0049] Según la presente invención, el contenido encriptado CT' y el valor aleatorio RV relevante se podrían usar como datos que deben guardarse, ya sea localmente dentro del mismo dispositivo que los había encriptado, o dentro de otro dispositivo (por ejemplo, el dispositivo 20), que está separado (o al menos es diferente) del primer dispositivo (dispositivo 10). Dicha situación podría ser útil, por ejemplo, para recuperar datos registrados en un primer dispositivo que se volvieron defectuosos si estos datos se enviaron previamente como copia de seguridad a un segundo dispositivo. Como ejemplo, si el chip 18 del primer dispositivo 10 se vuelve inservible, por cualquier razón, y sus datos (o datos almacenados en otro lugar en el dispositivo 10) se enviaron previamente a un segundo dispositivo 20 de una forma encriptada (CT') con el valor aleatorio RV relevante, entonces un nuevo dispositivo 10 (obtenido en sustitución del precedente) puede recuperar fácilmente los datos almacenados (después de que se haya realizado la fase de activación) pidiendo al segundo dispositivo 20 que envíe de nuevo el contenido encriptado CT' y el valor aleatorio RV correspondiente (si es necesario, junto con los datos de activación V, KN' correspondientes, sin excluir el envío directo de la clave de red KN, incluso si dicho senario es menos recomendable).

[0050] Ventajosamente, debe tenerse en cuenta que aunque la clave de red KN es una clave que es común a cada dispositivo 10, 20, esta clave de red nunca se expone fuera del chip 18, 28 de estos dispositivos. Además, fuera de los chips, las claves de red encriptadas KN'_1, KN'_2 parece que son ventajosamente distintas entre sí. Más ventajosamente, y conforme a la forma de realización preferida, todos los valores V_n, KN'_n, RV que pasan tanto a través de la red, como a través de cada dispositivo 10, 20 no permiten, por sí solos, desencriptar el contenido encriptado CT'. En consecuencia, cualquier piratería de dichos datos por parte de una persona malintencionada, incluso dentro del dispositivo 10, 20 o en la interfaz entre este dispositivo y la red, no tendrá ningún efecto sobre la seguridad del contenido intercambiado. Esta es una de las ventajas principales de la presente invención.

[0051] Además, gracias a las tres operaciones criptográficas sucesivas realizadas por los tres módulos criptográficos 11, 12, 13, la clave de contenido Kc se determinada basándose en dos claves K_1, KN, que se determinan, directa o indirectamente, a partir del valor secreto S. Ventajosamente, esta manera de hacerlo permite mantener el valor secreto S inaccesible para el centro de gestión, lo que evita cualquier riesgo de fuga de datos sensibles que pudiera corromper la seguridad del sistema.

[0052] Asimismo, las memorias 16, 26 de los chips 18, 28 se refieren cada una a una memoria segura en la que solo es posible escribir muy pocos datos y muy raramente. Esta restricción física de esta memoria integrada en el chip permite escribir una vez los datos raíz (es decir, el valor secreto S), y luego introducir dinámicamente en el chip varias claves asignadas a diferentes entidades del sistema.

[0053] Aun ventajosamente, la clave de red KN puede ser renovada fácilmente por el centro de gestión y, por lo tanto, el método de la presente invención no es un método estático, pero puede cambiar fácilmente con el tiempo.

[0054] Preferiblemente, las claves de dispositivo K (K_1, K_2, ... K_n) son generadas por el generador de clave 4 del centro de gestión 1. Sin embargo, también se podría usar otro generador de clave similar para este fin.

[0055] La presente invención también se refiere a un sistema para transferir un contenido CT de forma segura entre dispositivos 10, 20 dentro de una red. Este sistema comprende un centro de gestión 1 provisto de:

- la memoria 6 para almacenar, para cada dispositivo 10, 20, la clave de dispositivo K y el valor de dispositivo V; donde dicho valor de dispositivo V es el resultado de una operación criptográfica preliminar, que usa dicha clave de dispositivo K como datos de entrada encriptados por medio del valor secreto S relevante al dispositivo 10, 20; la clave de dispositivo K y el valor de dispositivo V se almacenan preferiblemente juntos dentro del registro asignado al dispositivo relevante; además, dado que los datos almacenados en la memoria 6 son datos sensibles, la memoria 6 es preferiblemente una memoria segura para proteger dichos datos contra cualquier intento de piratería; donde el valor secreto S, la clave de dispositivo K y el valor de dispositivo V son exclusivos y diferentes para cada uno de dichos dispositivos,

- el generador de clave 4 para generar la clave de red KN,

- el módulo de encriptación 5 para determinar, para cada dispositivo 10, 20, la clave de red encriptada KN', que es el resultado de la encriptación de la clave de red KN por medio de la clave de dispositivo K correspondiente, es decir, la clave de dispositivo K que pertenece al dispositivo 10, 20 relevante,

- la unidad 7 de envío para transmitir a cada dispositivo 10, 20 su valor de dispositivo V y su clave de red encriptada KN', es decir, el valor de dispositivo V y la clave de red encriptada KN' que pertenecen al dispositivo relevante,

donde cada uno de estos dispositivos 10, 20 comprende:

- al menos una interfaz de entrada/salida para recibir y enviar datos,

- la memoria segura 16, 26 para almacenar el valor secreto S preinicializado; donde esta memoria es típicamente una memoria de solo lectura,

- el primer módulo criptográfico 11, 21, que usa el valor de dispositivo V y el valor secreto S relevante a este dispositivo 10, 20 como entrada de un primer algoritmo criptográfico para generar la clave de dispositivo K,

- el segundo módulo criptográfico 12, 22, que usa la clave de red encriptada KN' y la clave de dispositivo K relevante a este dispositivo 10, 20 como entrada de un segundo algoritmo criptográfico para generar la clave de red KN,

- el generador de valor aleatorio 14, 24 para generar un valor aleatorio RV cuando dicho dispositivo actúa como dispositivo de envío 10 para transferir el contenido CT a al menos un otro dispositivo 20 de la red,

- el tercer módulo criptográfico 13, 23, que usa el valor aleatorio RV y la clave de red KN como entrada del tercer algoritmo criptográfico para generar la clave de contenido Kc,

- el módulo criptográfico de contenido 15, 25, que usa la clave de contenido Kc y el contenido CT, CT' como entrada del algoritmo criptográfico de contenido para generar el contenido encriptado CT' a partir del contenido CT de texto sencillo o el contenido CT de texto sencillo a partir del contenido encriptado CT' dependiendo de si el dispositivo actúa como dispositivo de envío o como dispositivo de recepción.

[0056] Para adaptarse también a la denominada "variante de transferencia CT" (figura 2), el tercer módulo criptográfico 13, 23 anteriormente mencionado y el módulo criptográfico de contenido 15, 25 anteriormente mencionado podrían definirse con otras palabras, de modo que el sistema de la presente invención comprende

- un tercer módulo criptográfico 13, 23, que usa el valor aleatorio RV y la clave de red KN como entrada de un tercer algoritmo criptográfico para generar una clave de contenido Kc; y un módulo criptográfico de contenido 15, 25, que usa dicha clave de contenido Kc y un contenido CT, CT' como entrada de un algoritmo criptográfico de contenido para generar un contenido encriptado CT' a partir de un contenido CT de texto sencillo o un contenido CT de texto sencillo a partir de un contenido encriptado CT',
  o

- un tercer módulo criptográfico 13, 23, que involucra el valor aleatorio RV, la clave de red KN y la clave de contenido Kc para obtener una clave criptográfica final por medio de un tercer algoritmo criptográfico; y

un módulo criptográfico de contenido 15, 25, que usa esta clave criptográfica final y un contenido CT, CT' como entrada de un algoritmo criptográfico de contenido para generar un contenido encriptado CT' a partir de un contenido CT de texto sencillo o un contenido CT de texto sencillo a partir de un contenido encriptado CT'.

[0057] Preferiblemente, y en otras palabras, cada uno de los dispositivos 10, 20 anteriormente mencionados del sistema comprende:

- al menos una interfaz de entrada/salida para recibir, desde el centro de gestión 1, el valor de dispositivo V y la clave de red encriptada KN' durante una fase de activación y para transferir datos, incluido el contenido CT durante una fase operativa posterior,
- una memoria segura 16, 26 para almacenar el valor secreto S preinicializado,
- un primer módulo criptográfico 11, 21, que usa el valor secreto S y el valor de dispositivo V para generar la clave de dispositivo K exclusiva,
- un segundo módulo criptográfico 12, 22, que usa la clave de dispositivo K para desencriptar la clave de red encriptada KN durante una fase de recuperación de claves,
- un generador de valor aleatorio 14 capaz de generar un valor aleatorio RV que se usará posteriormente (directa o indirectamente) como datos para la encriptación/desencriptación de contenido CT,
- un tercer módulo criptográfico 13, 23 para generar una clave final, o datos que se van a asociar al contenido encriptado (según la denominada "variante de transferencia CT"), durante una fase operativa al realizar una operación criptográfica que involucra el valor aleatorio RV y la clave de red KN, preferiblemente al encriptar o desencriptar dicho valor aleatorio RV por medio de dicha clave de red KN,
- un módulo criptográfico de contenido 15, 25, que usa la clave final para encriptar/desencriptar el contenido CT.

[0058] Según una forma de realización particular de este sistema, la memoria segura 16 o 26, el primer módulo criptográfico 11 o 21, el segundo módulo criptográfico 12 o 22, el tercer módulo criptográfico 13 o 23 y el módulo criptográfico de contenido 15 o 25 están incluidos dentro de un único chip 18 o 28 (es decir, un chip monolítico) situado en el dispositivo 10 o 20.

[0059] Según otra forma de realización, cada dispositivo 10, 20 comprende además una memoria no volátil 17. Esta memoria 17 se puede usar para almacenar los datos de activación V, KN' y/o el valor aleatorio RV en referencia a un cierto contenido encriptado CT'. Dependiendo del tamaño disponible de esta memoria no volátil 17, este contenido encriptado CT' también se podría almacenar en esta memoria no volátil o se puede almacenar en un medio de almacenamiento separado apropiado. Preferiblemente, esta memoria no volátil 17 (o 27) se usa para almacenar datos que no requieren un alto nivel de seguridad.

[0060] La presente invención finalmente también se refiere a un dispositivo para transferir contenido CT de forma segura con uno o varios otros dispositivos 10, 20, idénticos dentro de la red. Para este fin, este dispositivo comprende:

- al menos una interfaz de entrada/salida para recibir y enviar datos,
- la memoria segura 16, 26 para almacenar el valor secreto S preinicializado, donde esta memoria es típicamente una memoria de solo lectura,
- el primer módulo criptográfico 11, 21, que usa el valor de dispositivo V recibido desde el centro de gestión 1 y el valor secreto S (asignado y exclusivo de este dispositivo) como entrada de un primer algoritmo criptográfico para generar la clave de dispositivo K conocida por dicho centro de gestión 1; donde dicho valor de dispositivo V y dicha clave de dispositivo K son exclusivas del dispositivo,
- el segundo módulo criptográfico 12, 22, que usa, por un lado, la clave de red encriptada KN' recibida desde el centro de gestión 1 y, por otro lado, la clave de dispositivo K que pertenece a este dispositivo como entrada del segundo algoritmo criptográfico para generar la clave de red KN conocida por dicho centro de gestión 1,
- el generador de valor aleatorio 14 para generar un valor aleatorio RV, en particular cuando este dispositivo 10, 20 actúa como dispositivo de envío 10 para transferir el contenido CT a al menos uno de los otros dispositivos de la red,

- el tercer módulo criptográfico 13, 23, que usa el valor aleatorio RV y la clave de red KN como entrada del tercer algoritmo criptográfico para generar la clave de contenido Kc,

- el módulo criptográfico de contenido 15, 25, que usa la clave de contenido Kc y el contenido CT, CT' como entrada de un algoritmo criptográfico de contenido para generar un contenido encriptado CT' a partir de un contenido CT de texto sencillo o un contenido CT de texto sencillo a partir de un contenido encriptado CT', dependiendo de si el dispositivo actúa como dispositivo de envío o como dispositivo de recepción.

[0061] Para adaptarse también a la denominada "variante de transferencia CT" (figura 2), el tercer módulo criptográfico 13, 23 anteriormente mencionado y el módulo criptográfico de contenido 15, 25 anteriormente mencionado podrían definirse con otras palabras, de modo que el sistema de la presente invención comprende

- un tercer módulo criptográfico 13, 23, que usa el valor aleatorio RV y la clave de red KN como entrada de un tercer algoritmo criptográfico para generar una clave de contenido Kc; y un módulo criptográfico de contenido 15, 25, que usa dicha clave de contenido Kc y un contenido CT, CT' como entrada de un algoritmo criptográfico de contenido para generar un contenido encriptado CT' a partir de un contenido CT de texto sencillo o un contenido CT de texto sencillo a partir de un contenido encriptado CT',
  o

- un tercer módulo criptográfico 13, 23, que involucra el valor aleatorio RV, la clave de red KN y la clave de contenido Kc para obtener una clave criptográfica final por medio de un tercer algoritmo criptográfico; y un módulo criptográfico de contenido 15, 25, que usa esta clave criptográfica final y un contenido CT, CT' como entrada de un algoritmo criptográfico de contenido para generar un contenido encriptado CT’ a partir de un contenido CT de texto sencillo o un contenido CT de texto sencillo a partir de un contenido encriptado CT'.

[0062] En otras palabras, y según un aspecto más general, el dispositivo de la presente invención puede describirse como que comprende:

- al menos una interfaz de entrada/salida para recibir un valor de dispositivo V exclusivo y una clave de red encriptada KN durante una fase de activación, que involucra un centro de gestión 1, y para transferir datos que incluyen el contenido CT durante una fase operativa posterior, que involucra solo los dispositivos 10, 20 (es decir, excluyendo el centro de gestión 1 de la fase operativa),

- una memoria segura 16, 26 para almacenar un valor secreto S exclusivo preinicializado,

- un primer módulo criptográfico 11, 21, que usa el valor secreto S y el valor de dispositivo V para generar una clave de dispositivo K exclusiva,

- un segundo módulo criptográfico 12, 22, que usa la clave de dispositivo K para desencriptar la clave de red encriptada KN durante una fase de recuperación de claves,

- un generador de valor aleatorio 14 capaz de generar un valor aleatorio RV, que se usará posteriormente (directa o indirectamente) como datos para la encriptación/desencriptación del contenido CT,

- un tercer módulo criptográfico 13, 23 para generar una clave final, o datos que se van a asociar al contenido encriptado (según la denominada "variante de transferencia CT"), durante una fase operativa al realizar una operación criptográfica que involucra el valor aleatorio RV y la clave de red KN, preferiblemente al encriptar o desencriptar dicho valor aleatorio RV por medio de dicha clave de red KN,

- un módulo criptográfico de contenido 15, 25, que usa dicha clave final para encriptar/desencriptar el contenido CT.

[0063] Según una forma de realización particular, la memoria segura 16 o 26, el primer módulo criptográfico 11 o 21, el segundo módulo criptográfico 12 o 22, el tercer módulo criptográfico 13 o 23 y el módulo criptográfico de contenido 15 o 25 están incluidos dentro de un único chip 18 o 28 (es decir, un chip monolítico) situado en el dispositivo 10 o 20.

[0064] Según otra forma de realización, cada dispositivo 10, 20 también comprende una memoria no volátil 17, 27. Esta memoria 17, 27 se puede usar para almacenar los datos de activación V, KN' y/o el valor aleatorio RV en referencia a un cierto contenido encriptado CT'. Preferiblemente, esta memoria no volátil 17, 27 se usa para almacenar datos que no requieren un alto nivel de seguridad. Dependiendo del tamaño disponible de esta memoria no volátil, este contenido encriptado CT' también se podría almacenar en esta memoria no volátil.

REIVINDICACIONES

1. Método para transferir un contenido CT de forma segura entre dispositivos (10, 20) dentro de una red, donde cada dispositivo (10, 20) comprende un valor secreto S exclusivo preinicializado, que es diferente para cada dispositivo, donde dicho método comprende:

una fase de activación que comprende los pasos de:

- generar, por un centro de gestión (1), una clave de red KN común a todos los dispositivos mencionados (10, 20),
- calcular, por el centro de gestión (1), una clave de red encriptada KN' para cada dispositivo (10, 20) al encriptar dicha clave de red KN usando una clave de dispositivo K, que es diferente para cada dispositivo (10, 20),
- transmitir, por el centro de gestión (1), a cada uno de dichos dispositivos (10,20), la clave de red encriptada KN' y un valor de dispositivo V resultante de una operación criptográfica preliminar destinada a encriptar la clave de dispositivo K de dicho dispositivo (10, 20) usando su valor secreto S,

una fase de recuperación de claves realizada por cada uno de dichos dispositivos (10, 20) y que comprende los pasos de:

- realizar una primera operación criptográfica para obtener la clave de dispositivo K a partir del valor de dispositivo V y del valor secreto S de dicho dispositivo (10, 20),
- realizar una segunda operación criptográfica para obtener la clave de red KN a partir de la clave de red encriptada KN' y de la clave de dispositivo K,

una fase operativa realizada por cada dispositivo (10, 20) involucrado en la transferencia de dicho contenido CT y dichos datos asociados, que comprende los siguientes pasos, que incluyen una tercera operación criptográfica realizada antes de encriptar o desencriptar dicho contenido CT,

- generar un valor aleatorio RV, que se usará posteriormente como datos para la desencriptación/encriptación de dicho contenido CT

si dicho contenido CT debe ser encriptado:

- usar un valor aleatorio RV y la clave de red KN como entradas de dicha tercera operación criptográfica,
- usar el resultado de dicha tercera operación criptográfica o dicho valor aleatorio RV como clave final para encriptar dicho contenido CT, y respectivamente
- usar dicho valor aleatorio RV o el resultado de dicha tercera operación criptográfica como datos asociados;

si dicho contenido CT debe ser desencriptado:

- usar dichos datos asociados y dicha clave de red KN como entradas de dicha tercera operación criptográfica,
- usar el resultado de dicha tercera operación criptográfica como clave final para desencriptar dicho contenido CT.

2. Método según la reivindicación 1, donde dicho valor secreto S es implementado de antemano en una memoria segura (16, 26), situada dentro de un chip (18, 28) del dispositivo (10, 20), por una autoridad de personalización (30).

3. Método según la reivindicación 2, donde dicha operación criptográfica preliminar es realizada por la autoridad de personalización (30).

4. Método según cualquiera de las reivindicaciones precedentes, donde las operaciones criptográficas primera, segunda y tercera se realizan con la encriptación o desencriptación del contenido CT dentro de un único chip (18, 28) en el dispositivo (10, 20).

5. Método según cualquiera de las reivindicaciones precedentes, donde dicha clave final se almacena en una memoria no volátil (17, 27) asociada a cualquiera de dichos dispositivos (10, 20).

6. Método según la reivindicación 5, donde el valor de dispositivo V y la clave de red encriptada KN' se almacenan en dicha memoria no volátil (17, 27).

7. Sistema para transferir un contenido CT de forma segura entre dispositivos (10, 20) dentro de una red, que comprende:

un centro de gestión (1) provisto de:

- una memoria (6) para almacenar, para cada dispositivo (10, 20), una clave de dispositivo K y un valor de dispositivo V, donde dicho valor de dispositivo V es el resultado de una operación criptográfica preliminar, que usa dicha clave de dispositivo K como datos de entrada encriptados usando un valor secreto S relevante a dicho dispositivo (10, 20), donde dicho valor secreto S, dicha clave de dispositivo K y dicho valor de dispositivo V son exclusivos y diferentes para cada dispositivo,
- un generador de clave (4) para generar una clave de red KN,
- una encriptación de módulo (5) para determinar, para cada dispositivo (10, 20), una clave de red encriptada KN', que es el resultado de la encriptación de la clave de red KN usando la clave de dispositivo K relevante a dicho dispositivo (10, 20),
- un unidad de envío (7) para transmitir a cada dispositivo (10, 20) su valor de dispositivo V y su clave de red encriptada KN',

donde cada uno de dichos dispositivos (10, 20) comprende:

- al menos una interfaz de entrada/salida para recibir, desde dicho centro de gestión (1), dicho valor de dispositivo V y dicha clave de red encriptada KN' durante una fase de activación y para transferir datos que incluyen dicho contenido CT durante una fase operativa posterior,
- una memoria segura (16, 26) para almacenar dicho valor secreto S preinicializado,
- un primer módulo criptográfico (11, 21), que usa dicho valor secreto S y dicho valor de dispositivo V para generar una clave de dispositivo K exclusiva,
- un segundo módulo criptográfico (12, 22), que usa dicha clave de dispositivo K para desencriptar dicha clave de red encriptada KN durante una fase de recuperación de claves,
- un generador de valor aleatorio (14) capaz de generar un valor aleatorio RV que se usará posteriormente como datos para la desencriptación/encriptación de dicho contenido CT,
- un tercer módulo criptográfico (13, 23) configurado para:

  recibir un valor aleatorio RV y dicha clave de red KN como entradas y generar un resultado a partir de su entrada si dicho contenido CT debe ser encriptado;
  y recibir dicha clave de red KN y los datos transferidos asociados a dicho contenido CT, donde dichos datos asociados a dicho contenido comprenden dicho valor aleatorio RV o dicho resultado a partir de dicho tercer módulo criptográfico, como entradas si dicho contenido CT debe ser desencriptado,
  donde dicho tercer módulo criptográfico (13, 23) proporciona una clave final como salida de cualquier par de entradas,

- un módulo criptográfico de contenido (15, 25) configurado para usar dicha salida o dicho valor aleatorio RV como clave final para encriptar dicho contenido CT,
  y para usar dicha salida como clave final para desencriptar dicho contenido CT.

8. Sistema según la reivindicación 7, donde cada uno de dichos dispositivos (10, 20) comprende un único chip (18, 28), que incluye dicha memoria segura (16, 26), dicho primer módulo criptográfico (11, 21), dicho segundo módulo criptográfico (12, 22), dicho tercer módulo criptográfico (13, 23) y dicho módulo criptográfico de contenido (15, 25).

9. Sistema según la reivindicación 7 o 8, donde este también comprende una memoria no volátil (17, 27) para almacenar datos que no requieren un alto nivel de seguridad.

10. Dispositivo (10) para transferir un contenido CT de forma segura a un segundo dispositivo (20) dentro de una red, que comprende:

- al menos una interfaz de entrada/salida para recibir un valor de dispositivo V exclusivo y una clave de red encriptada KN durante una fase de activación, que involucra un centro de gestión (1) y para transferir datos, que incluyen dicho contenido CT durante una fase operativa posterior, que involucra solo dichos dispositivos (10, 20),
- una memoria segura (16, 26) para almacenar un valor secreto S exclusivo preinicializado,
- un primer módulo criptográfico (11, 21), que usa dicho valor secreto S y dicho valor de dispositivo V para generar una clave de dispositivo K exclusiva,
- un segundo módulo criptográfico (12, 22), que usa dicha clave de dispositivo K para desencriptar dicha clave de red encriptada KN durante una fase de recuperación de claves,
- un generador de valor aleatorio (14) capaz de generar un valor aleatorio RV, que se usará posteriormente como datos para la encriptación/desencriptación de dicho contenido CT,
- un tercer módulo criptográfico (13, 23) configurado para:

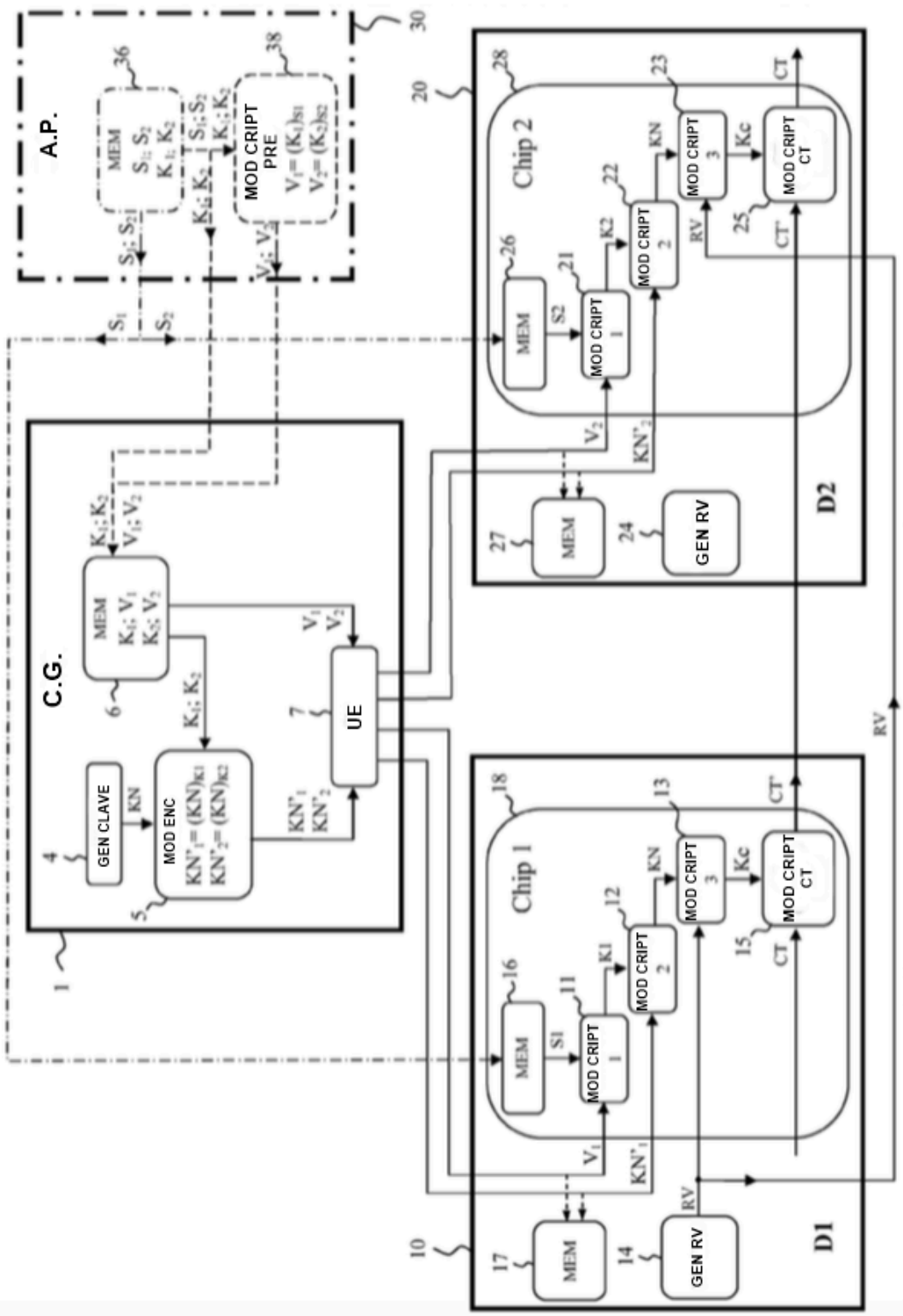
recibir un valor aleatorio RV y dicha clave de red KN como entradas y
generar un resultado a partir de su entrada si dicho contenido CT debe ser encriptado;
y recibir dicha clave de red KN y los datos transferidos asociados a dicho contenido CT, donde dichos datos asociados a dicho contenido comprenden dicho valor aleatorio RV o dicho resultado a partir de dicho tercer módulo criptográfico, como entradas si dicho contenido CT debe ser desencriptado,
donde dicho tercer módulo criptográfico (13, 23) proporciona una clave final como salida de cualquier par de entradas,

- un módulo criptográfico de contenido (15, 25) configurado para usar dicha salida o dicho valor aleatorio RV como clave final para encriptar dicho contenido CT, y para
usar dicha emisión como clave final para desencriptar dicho contenido CT.

11. Dispositivo según la reivindicación 10, donde este comprende un único chip (18, 28), que incluye dicha memoria segura (16, 26), dicho primer módulo criptográfico (11, 21), dicho segundo módulo criptográfico (12, 22), dicho tercer módulo criptográfico (13, 23) y dicho módulo criptográfico de contenido (15, 25).

12. Dispositivo según la reivindicación 10 o 11, donde este también comprende una memoria no volátil (17, 27) para almacenar datos que no requieren un alto nivel de seguridad.

Fig. 1


A.P.
MEM
MOD CRIPT PRE
C.G.
GEN CLAVE
MOD ENC
UE
Chip 1
Chip 2
MOD CRIPT 1
MOD CRIPT 2
MOD CRIPT 3
MOD CRIPT CT
GEN RV
D1
D2

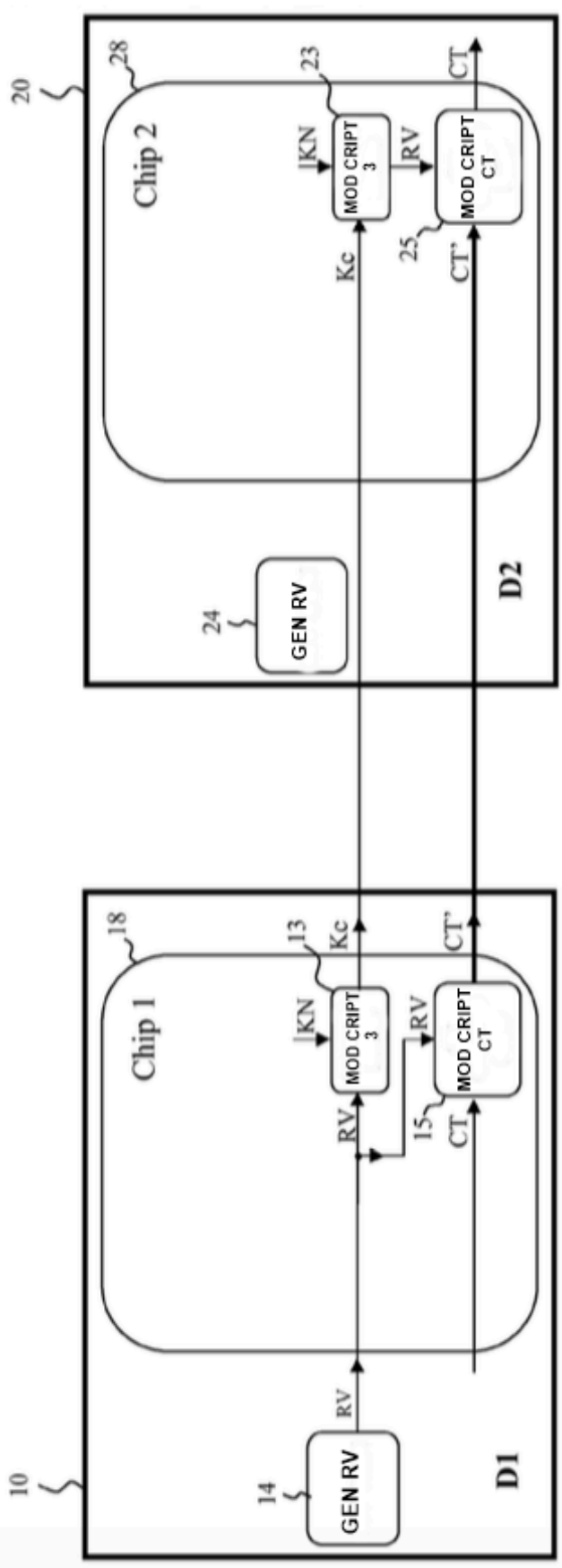

10
D1
GEN RV
14
RV
Chip 1
18
MOD CRIPT 3
13
KN
RV
MOD CRIPT CT
15
CT
Kc
CT'
20
D2
GEN RV
24
Chip 2
28
MOD CRIPT 3
23
KN
RV
MOD CRIPT CT
25
CT
Kc
CT'

Fig. 2