(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 661 059**

(51) Int. CI.:

G06F 21/00 (2013.01)
H04L 9/12 (2006.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **31.12.2010 PCT/EP2010/070950**

(87) Fecha y número de publicación internacional: **14.07.2011 WO11083069**

(96) Fecha de presentación y número de la solicitud europea: **31.12.2010 E 10800964 (8)**

(97) Fecha y número de publicación de la concesión europea: **06.12.2017 EP 2521984**

(54) Título: **Procedimiento de protección de contenidos y de servicios multimedia**

(30) Prioridad:

05.01.2010 FR 1050035

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.03.2018

(73) Titular/es:

VIACCESS (100.0%)
Les Collines de l'Arche Tour Opéra C
F-92057 Paris La Defense Cedex, FR

(72) Inventor/es:

NEAU, LOUIS

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Procedimiento de protección de contenidos y de servicios multimedia

Campo técnico

La invención se sitúa en el campo de la protección de contenidos y se dirige más específicamente a la protección de contenidos y de servicios multimedia distribuidos por un operador a diversos abonados provistos de terminales de recepción adaptados para este fin.

La invención se refiere igualmente a un terminal de recepción adaptado para recibir dichos contenidos y servicios y a un programa de ordenador memorizado sobre un soporte de registro y adaptado para implementar el procedimiento cuando se ejecuta por un ordenador.

El procedimiento se aplica a los contenidos protegidos suministrados a unos terminales tales como descodificadores, ordenadores o teléfonos móviles y se dirige, principalmente, a mejorar la protección de los modelos económicos de los operadores y de los suministradores de tecnologías de protección de contenidos evitando la redistribución ilícita de estos contenidos.

Estado de la técnica anterior

La figura 1 ilustra esquemáticamente una arquitectura clásica para suministrar contenidos codificados mediante una plataforma de codificación 2 a un terminal 4 conectado a la red de un operador.

Una arquitectura de ese tipo de suministro de contenido, asegura normalmente la protección del contenido a transmitir 6, previamente codificado, del lado del operador, por un módulo de codificación 8 que utiliza una clave de contenido CW.

La clave de contenido se cifra a continuación por medio de una clave de acceso al contenido K, mediante la aplicación de una función F, y posteriormente se transmite, en la forma de un criptograma CW*, por el operador a un agente 10 de control de acceso al contenido dispuesto en el terminal 4.

Pueden transmitirse unas condiciones que definen unos usos autorizados de dicho contenido al terminal paralelamente a la clave de acceso al contenido K.

La revelación de la clave de acceso al contenido K por el agente 10, con el fin de su suministro al módulo de descodificación 12 del terminal 4, se somete a la obtención previa, por este agente 10, de un derecho de acceso al contenido que se materializa generalmente como mínimo por la obtención de la clave de acceso al contenido K.

La clave de acceso al contenido K obtenida por el agente 10 se utiliza a continuación para descifrar el criptograma de la clave de contenido mediante la aplicación de la función F^{-1}, inversa de la función F, y revelar así la clave de contenido CW. Esta se suministra a continuación al módulo de descodificación 12, dispuesto en el terminal 4.

La clave de contenido CW puede renovarse regularmente con el tiempo, principalmente para los contenidos lineales como por ejemplo según un cripto-período preestablecido, normalmente de 10 segundos en unos flujos difundidos.

Esta protección del contenido se implementa generalmente por un sistema de acceso condicional, o CAS, por Conditional Access System, o mediante el sistema de gestión de derechos digitales, o DRM, por Digital Rights Management. En lo que sigue de la presente descripción, las características y funciones de dichos sistemas, bien conocidos para el experto en la materia, no se describirán más en detalle. Para más informaciones, el lector puede dirigirse por ejemplo a los documentos siguientes:

- sobre los sistemas de acceso condicional, “Functional Model of Conditional Access System”, EBU Review, Technical European Broadcasting Union, Bruselas, BE, n.º 266, 21 de diciembre de 1995;
- sobre los sistemas de gestión de los derechos digitales, “DRM Specification”, Open Mobile Alliance OMA-TS-DRMDRM-V2_0_2-20080723-A, la versión aprobada 2.0.2 - 23 de julio de 2008.

Además de la protección del contenido, una arquitectura de este tipo de suministro de contenidos asegura una protección del servicio de suministro de dicho contenido. Esta protección se asegura generalmente por el agente de control 10 y por un cargador de inicio controlado (por boot loader en inglés). Estos dos elementos se basan normalmente en las funciones de seguridad de un circuito integrado (chipset) del terminal, según la disponibilidad de estas funciones en el circuito integrado elegido.

La protección del servicio consiste principalmente en asegurar la conformidad funcional de los procesamientos realizados por las entidades del sistema, y principalmente del terminal, y unos datos de configuración utilizados por estos últimos, respectivamente a los procesamientos y a los datos previstos por el operador.

Puede por ejemplo tratarse de asegurar la activación de la protección de la memoria, o la implementación de soluciones de anti-volcado o anti-depuración, que se dirigen a impedir la observación de la ejecución del programa informático que realiza la descodificación de los contenidos en el terminal.

La protección del servicio se basa normalmente en unas técnicas criptográficas y está fundada más generalmente en la implementación de funciones de seguridad establecidas durante las fases de concepción o de integración del terminal. Estas se traducen por ejemplo en unas exigencias transmitidas por el suministrador de tecnologías de protección de contenidos, o del operador de servicios de contenido, hacia las industrias encargadas de fabricar los circuitos integrados o los terminales afectados.

El respeto a estas exigencias puede verificarse principalmente por medio de un proceso de validación o de certificación sobre una muestra muy limitada de terminales antes de su envío al mercado.

La protección del contenido y la protección del servicio son complementarias en el seno de la arquitectura de suministro de contenidos, para asegurar un suministro eficaz del contenido. Aunque lógicamente relacionadas, estas protecciones no están generalmente relacionadas en sus ejecuciones. En efecto, el no respeto de las exigencias de seguridad o de la política de seguridad de servicio, normalmente el puerto JTAG abierto, el control de integridad del código no activado, la ausencia de la desactivación de las salidas no autorizadas (HDD, salidas analógicas,…), o una versión no actualizada de todo o parte del entorno de software, no impiden la revelación de la clave de contenido y el aprovechamiento de este contenido.

Obsérvese que el problema de la redistribución de las claves de contenido CW es actualmente uno de los fallos fundamentales de los sistemas de suministro de contenidos. La resistencia y la renovación del aseguramiento de la protección de la clave de contenido CW desde la cabecera de la red hasta su utilización a nivel del módulo de descifrado del circuito integrado del terminal continúa siendo un problema fundamental.

Por otro lado, en el caso de una difusión amplia de contenidos a un parque de terminales de recepción, la implementación efectiva de las exigencias de seguridad y de la política de seguridad del servicio no puede verificarse de manera dinámica sobre el conjunto del parque de terminales. Ahora bien el no respeto de estas exigencias en uno solo de los terminales puede poner en peligro potencialmente a todo el modelo económico del operador.

Por otro lado, la presentación de la oferta puede incluir por ejemplo publicidad o unos enlaces hacia otros servicios anexos, tales como los servicios asociados al suministro del contenido, unos artilugios o unos servicios de comunicación, que pueden ser también importantes para el operador. Este último puede así diferenciarse de la competencia ofreciendo una experiencia de usuario propia.

Es en consecuencia igualmente imperativo proteger, además del contenido, la presentación de la oferta y los servicios asociados.

Un objetivo de la invención es relacionar en sus ejecuciones la protección de los contenidos suministrados por un operador a la protección del servicio que soporta su suministro, comprendido en ella la presentación de la oferta y unos servicios asociados, con el fin de asegurar la permanencia del modelo económico del operador.

En lo que sigue del documento, se habla de sobre-cifrado, cuando el dato a proteger se cifra al menos dos veces por medio de algoritmos de cifrado simétricos o asimétricos comunes o distintos y al menos dos claves distintas respectivamente secretas o públicas.

El documento FR 2 922 585 se refiere a un procedimiento de difusión, por medio de una red de banda ancha, de un programa multimedia codificado en el que se puede encaminar una información hacia una dirección de multidifusión de manera que solo un grupo de varios terminales correspondientes a esta dirección multidifusión recibe la información mientras que otros terminales conectados a la misma red no reciben esta información.

El documento FR 2 922 585 se refiere a un procedimiento de obtención por una primera entidad U de un valor derivado K_r, a partir de un parámetro de entrada r y de informaciones cifradas con el fin de trazar la primera entidad.

Exposición de la invención

Este objetivo se alcanza por medio de un procedimiento de protección de un contenido codificado mediante una clave de contenido CW transmitida cifrada por medio de una clave K de acceso al contenido mediante la aplicación de la función F, siendo suministrado dicho contenido por un sistema de emisión a al menos un terminal de recepción por medio de un servicio configurado localmente a nivel de dicho terminal de recepción según un conjunto de propiedades Pi, i = 1 a N, conocidas por el sistema de emisión, siendo representadas cada una de dichas propiedades Pi por un dato x_i memorizado en dicho sistema de emisión y por un dato y_i local y accesible para lectura a dicho terminal.

El procedimiento según la invención incluye en la emisión una etapa que consiste en sobre-cifrar dicha clave de contenido CW mediante al menos una función invertible de sobre-cifrado $f_i(x_i)$ dependiente de al menos unas propiedades Pi, i=1 a n.

Según un modo preferido de implementación, este procedimiento incluye las etapas siguientes:

en la emisión

- definir un subconjunto EP no vacío de propiedades Pi, i = 1 a n, a verificar,
- sobre-cifrar dicha clave de contenido CW aplicando sobre dicha clave de contenido CW las funciones invertibles de sobre-cifrado $f_i(x_i)$ para cada propiedad Pi, i = 1 a n, de dicho subconjunto EP,
- transmitir dicha clave de contenido CW sobre-cifrada al terminal (4),

y en la recepción,

- para cada propiedad Pi que pertenece a dicho subconjunto EP, leer el dato local y_i de dicho terminal que representa dicha propiedad Pi,
- revelar el valor CW' de dicha clave de contenido CW sobre-cifrada aplicando sobre dicha clave de contenido CW sobre-cifrada las funciones inversas de sobre-cifrado $f_i^{-1}(y_i)$ para cada una de las propiedades Pi de dicho subconjunto EP i = n a 1,
- descodificar el contenido por medio de la clave de contenido revelada.

Obsérvese que $f_i(x_i)$ y $f^{-1}(y_i)$ son unas funciones inversas para un par de valores (x_i, y_i) predeterminados, par en el que cada miembro representa la propiedad Pi de servicio respectivamente en el sistema de emisión y en el terminal de recepción. De ese modo, para un sobre-cifrado de la clave de contenido CW por una al menos de dichas funciones invertibles de sobre-cifrado $f_i(x_i)$ calculada en el sistema de emisión, si el dato y_i leído localmente en el receptor es diferente del valor esperado, la función inversa de sobre-cifrado $f^{-1}(y_i)$ calculada en la recepción y aplicada a la clave de contenido CW sobre-cifrada será falsa. En este caso, no se revela la clave de contenido CW, y se obtiene un valor CW', diferente de CW. El descodificador, que utiliza este valor CW' para tratar el contenido codificado, no podrá por tanto descodificarlo. La no conformidad de la propiedad Pi considerada del servicio impide por tanto la revelación correcta de la clave CW de contenido, y por tanto la descodificación de esta.

También, si en la emisión, se tienen en cuenta varias propiedades P_i, i = 1 a n, estas estarán, en la recepción, en orden inverso, es decir para i variando de n a 1.

Si uno al menos de los pares predefinidos (x_i, y_i) que representan las propiedades Pi no está conforme, las funciones de sobre-cifrado respectivas $f_i(x_i)$ y $f^{-1}(y_i)$ no están ya en relación inversa y en consecuencia la revelación de la clave de contenido CW, así como el descodificación del contenido, son erróneos.

En el modo de realización preferido presentado, el sobre-cifrado realizado de la clave CW de contenido con al menos una función de sobre-cifrado $f_i(x_i)$ característica de la propiedad Pi del servicio, es un pre-cifrado en el sentido en el que interviene, en el procedimiento según la invención, antes del cifrado con la clave K de acceso al contenido según la técnica anterior. En una variante de la invención, este sobre-cifrado se realiza después del cifrado con la clave K de acceso al contenido, y constituye de ese modo un post-cifrado.

En los modos de realización de la invención que requieren varios sobre-cifrados, estos podrán, según otra variante de la invención, incluir al menos un pre-cifrado y al menos un post-cifrado tal como se han definido anteriormente.

Preferentemente, la clave de contenido CW no se revela más que después de tener en cuenta el conjunto de las propiedades P_i, i = 1 a n. En la emisión, la clave de contenido CW sobre-cifrada se transmite al terminal de manera síncrona con una lista de referencias que representan un subconjunto EP de las propiedades P_i del servicio a verificar, correspondientes a los datos x_i, i = 1 a n, utilizados para calcular las funciones de sobre-cifrado $f_i(x_i)$, y a los datos y_i, i = 1 a n, utilizados para el cálculo por el terminal de las funciones inversas de sobre-cifrado $f_i(y_i)$, y en la recepción, el terminal aplica sucesivamente las funciones inversas $f_i^{-1}(y_i)$ sobre la clave de contenido sobre-cifrada CW y obtiene como resultado la clave revelada CW', para i variando de n a 1.

La toma en consideración de las propiedades P_i, i = 1 a n, se realiza sistemáticamente o de manera puntual.

La invención se implementa mediante una plataforma de codificación de un contenido codificado por una clave de contenido CW cifrada mediante una clave de acceso al contenido K y suministrada con al menos un servicio por un operador a al menos un terminal de recepción, que incluye:

- unos medios para configurar dicho servicio para un conjunto que comprende un número entero de datos de configuración x_i, i = 1 a n, definiendo cada uno una propiedad Pi, i = 1 a n, de un contexto de implementación de dicho servicio por el terminal,
- unos medios para cifrar dicha clave de contenido CW mediante al menos un valor digital de cifrado calculado en

función de al menos un dato de configuración x_i, i = 1 a n.

En el lado de recepción, el contenido se descodifica mediante una plataforma de descodificación que incluye:

- unos medios para encontrar cada valor digital de cifrado x_i, i = 1 a n, por medio de la función f_i^{-1}, inversa de la función f_i, i = 1 a n,
- unos medios para descifrar la clave de contenido CW,
- unos medios para descodificar el contenido por medio de la clave de contenido CW.

Obsérvese que el procedimiento según la invención permite utilizar los parámetros de configuración en hardware y/o software del servicio que soporta el suministro del contenido disponible a nivel del terminal, no solamente para verificar la configuración de este servicio, sino también para generar al menos una clave de sobre-cifrado del contenido suministrado de manera que todas las modificaciones de dichos parámetros de configuración del servicio conduzcan a una clave de contenido errónea.

La indicación de la conformidad o no del servicio en este caso no es por tanto más que una consecuencia del procedimiento según la invención, que tiene además la ventaja de no presentar las vulnerabilidades conocidas a los ataques de las bifurcaciones lógicas de ensayos condicionales.

Breve descripción de los dibujos

Surgirán otras características y ventajas de la invención con la descripción que sigue, tomada a título de ejemplo no limitativo, con referencia a las figuras adjuntas en las que:

- la figura 1 ilustra esquemáticamente una arquitectura clásica para la distribución de contenidos codificados por un operador a unos terminales conectados al operador a través de una red de comunicación,
- la figura 2 ilustra esquemáticamente una primera variante de implementación del procedimiento en la arquitectura de la figura 1,
- la figura 3 ilustra esquemáticamente una segunda variante de implementación del procedimiento en la arquitectura de la figura 1.

Exposición detallada de modos de realización particulares

En lo que sigue de la descripción, se utilizarán unas referencias idénticas para designar los elementos comunes a la figura que ilustra la arquitectura de la técnica anterior y las diferentes figuras que ilustran la invención.

La figura 2 ilustra esquemáticamente el principio general de la invención que consiste en relacionar la revelación de la clave de contenido CW a uno o varios datos de configuración x_i, i = 1 a n, del servicio suministrado por el operador.

Con este fin, como se ilustra en la figura 2, la plataforma de codificación 2 incluye una unidad 20 de sobre-cifrado de la clave de contenido CW previamente a su cifrado por una clave de acceso al contenido K, que comprende n submódulos de sobre-cifrado 22_i, i = 1 a n, comprendiendo cada submódulo 22_i una rutina destinada a aplicar selectivamente a la clave CW cifrada una función invertible f_i, i = 1 a n, teniendo como parámetro de entrada un dato x_i, i = 1 a n, representativo de una propiedad P_i, i = 1 a n, de un contexto de implementación de dicho servicio por el terminal 4. Se denotará $f_i(x_i)$ esta función invertible de sobre-cifrado.

Obsérvese que las propiedades del servicio P_i, i = 1 a n, se representan, en la emisión por los valores x_i especificados por el operador, y en la recepción por sus valores efectivos y_i obtenidos por medición o por cálculo en el entorno del terminal 4.

El terminal 4 incluye, además del agente de control de acceso 10, una unidad de cálculo 40 destinada a aplicar selectivamente a la clave CW sobre-cifrada la función de sobre-cifrado inversa $f_i^{-1}(y_i)$, i = 1 a n, inversa de la función $f_i(x_i)$, i = 1 a n, utilizada en la emisión para sobre-cifrar la clave CW. Cuando x_i e y_i están de acuerdo con los valores esperados, $f_i^{-1}(y_i)$ ($f_i(x_i)$ (CW)) = CW, llegado el caso, las dos funciones $f_i(x_i)$ y $f_i^{-1}(y_i)$ no están en relación inversa.

La unidad de cálculo 40 incluye n submódulos de procesamiento 42_i, i = 1 a n, destinados a aplicar a la clave de contenido CW descifrada por medio de la función F^{-1} y al menos una función $f_i^{-1}(y_i)$, i = 1 a n, inversa de la función de sobre-cifrado $f_i(x_i)$, i = 1 a n, aplicada en la plataforma de codificación 2.

El agente de control de acceso 10 se configura para suministrar la clave de acceso al contenido K y los datos y_i, i = 1 a n, correspondientes a los datos x_i utilizados por la plataforma de codificación para calcular la clave de sobre-cifrado $f_i(x_i)$, i = 1 a n.

Con este fin, el operador transmite el terminal 4 una referencia del (o de los) datos x_i, i = 1 a n, que han servido, en la emisión, para el cálculo de la clave de sobre-cifrado $f_i(x_i)$, i = 1 a n. Las referencias EP corresponden al

subconjunto de las propiedades de servicio Pi que se desea verificar.

En la recepción de este subconjunto EP de referencias, el terminal 4 determina, mediante cálculo o medición, los valores corrientes y_i, i = 1 a n, correspondientes a las referencias trasmitidas y aplica una a una las funciones inversas $f_i^{-1}(y_i)$ en el orden i = n a 1 sobre la clave CW sobre-cifrada. Se obtiene así un resultado CW'.

Si los valores corrientes y_i, i = 1 a n corresponden respectivamente a los valores esperados por el operador, entonces se revela el valor de la clave de contenido CW por CW' y permite la descodificación del contenido (siendo CW igual a CW').

Si no, el valor de la clave de contenido CW' es falso y la descodificación conduce a un resultado incomprensible (siendo CW diferente de CW') en lo que sigue de la cadena de procesamiento del contenido, normalmente la descodificación.

Se ha de observar que el procedimiento según la invención permite forzar al terminal a tener en cuenta las propiedades P_i, i = 1 a n, del servicio antes de permitir la utilización del contenido.

Se ha de observar igualmente que si la clave de contenido CW evoluciona con el transcurso del tiempo, caso principalmente de los contenidos difundidos o en "directo", los valores x_i, i = 1 a n, pueden ajustarse para cada envío de la clave de contenido CW en función de las modificaciones aportadas al servicio o a los comportamientos esperados del terminal 4.

Por otro lado, la conformidad de las propiedades P_i, i = 1 a n, puede verificarse sistemáticamente o de manera puntual, incluso aleatoria. Si la verificación de una propiedad *Pi* es sistemática, entonces el cálculo del valor *yi* en el lado del terminal puede llegar a ser implícito y por tanto la referencia a *Pi* no tiene necesidad de transmitirse al terminal.

Además, las propiedades verificadas deben estar de acuerdo con el tipo de difusión del contenido. Además, si una clave de contenido CW se difunde de manera amplia sobre un conjunto de terminales, entonces los datos esperados y_i, i = 1 a n, representativos respectivamente de las propiedades del servicio P_i, i = 1 a n, deben tener las mismas representaciones respectivas sobre el conjunto del parque de terminales objetivo. Dichos datos y_i, i = 1 a n, tienen unos valores accesibles directamente o que pueden ser resultado de una medición o de un cálculo previo (hash,…). Pueden representar una única propiedad o una combinación de propiedades coherentes del servicio. Deben estar igualmente formateados de manera que se utilicen correctamente por las funciones inversas de sobre-cifrado $f_i^{-1}(y_i)$, i = n a 1, de la clave de contenido CW a la que están asociadas.

Estas funciones $f_i(x_i)$ y $f_i^{-1}(y_i)$ i = 1 a n, pueden reposar sobre las funciones criptográficas estándar o propietarias. Su complejidad tiene en cuenta un compromiso entre el nivel de protección esperado y el rendimiento de los terminales. Pueden presentarse en forma de funciones relativamente simples, tales como una adición XOR, una permutación o una sustitución, o incluso en la forma de algoritmos complejos tales como 3-DES o AES. Los valores x_i e y_i pueden representar un mismo estado de la propiedad Pi con unos valores digitales diferentes aunque equivalentes. En este caso, $f_i(x_i)$ y $f_i^{-1}(y_i)$ integran unas operaciones de cálculo de reformateo de los datos que lleva a una estricta igualdad entre x_i e y_i y permite de ese modo una definición simple de $f_i^{-1}(y_i)$ a partir de $f_i(x_i)$.

La sintaxis de las referencias EP de los datos x_i, i = 1 a n, trasmitidos al terminal 4 puede protegerse con el fin de enmascarar, en la mensajería, P_i, i = 1 a n, que el operador desea utilizar. En este caso, puesto que las referencias no cambian forzosamente con cada cambio de la clave de contenido, las referencias transmitidas pueden concatenarse aleatoriamente renovadas con cada cambio de la clave de contenido. El criptograma de las referencias es de ese modo diferente para cada clave de contenido.

La figura 3 ilustra esquemáticamente la implementación del procedimiento según la invención en un entorno en el que coexisten dos módulos de seguridad, el módulo de seguridad del chipset de un descodificador 50 y el chipset de seguridad de la tarjeta de chips 52.

En este tipo de entorno, el operador puede repartir las propiedades a utilizar entre los diferentes módulos según el orden de paso del criptograma de la clave de contenido CW en estos módulos. Ciertas propiedades pueden aplicarse igualmente por uno de los módulos para verificar la conformidad del comportamiento del otro módulo.

El procedimiento según la invención puede implementarse igualmente en la comunicación entre dos de dichos módulos, tal como por ejemplo un módulo de recepción de contenido considerado como punto de emisión y un procesador de seguridad asociado considerado como punto de recepción en el sentido del procedimiento según la invención. Las referencias de las propiedades a verificar deben ser respectivamente conocidas por (o transmitidas a) cada uno de los módulos afectados. El conjunto de las propiedades no tiene necesidad de circular sobre el conjunto de las interfaces entre los diferentes módulos.

Con referencia a la figura 3, la plataforma de codificación 2 incluye un submódulo de sobre-cifrado 22 que comprende una rutina destinada a aplicar a la clave CW cifrada una función f_1, que tiene por parámetros de entrada un dato x_1 *denotada* $f_i(x_i)$, representativo de la propiedad P_1 de configuración del módulo de seguridad del chipset del descodificador 50. El descodificador 50 dispone en la lectura del dato y_1 correspondiente a P_1. Este último incluye un submódulo de procesamiento 42 destinado a aplicar a la clave de contenido CW la función $f^{-1}(y_1)$, inversa de la función $f_1(x_1)$, aplicada en la plataforma de codificación 2 que tiene como entrada el valor y_1 suministrado por el chipset del descodificador.

En el lado del terminal 4, el chipset del descodificador 50 incluye una unidad de cálculo 40 que incluye un submódulo de procesamiento 42_1 destinado a aplicar a la clave CW sobre-cifrada la función $f^{-1}{}_1(y_1)$, inversa de la función f_1, utilizada en la emisión para sobre-cifrar la clave CW.

Si el dato y_1 suministrado por el chipset del descodificador 50 no es coherente con el dato x_1 utilizado a la altura de la plataforma de codificación como entrada de la función f_1, esto significará que la propiedad P_1 configurada por el operador no se respeta. En este caso, el valor de la clave de contenido CW no se revela por el desciframiento operado y la descodificación conduce a un resultado incomprensible en lo que sigue de la cadena de procesamiento del contenido, normalmente la descodificación.

Por otro lado, en el ejemplo ilustrado en la figura 3, la plataforma de codificación 2 incluye al menos un submódulo de sobre-cifrado 22_k que comprende una rutina destinada a aplicar a la clave CW una función f_k, que tiene por parámetros de entrada un dato x_k, representativo de una propiedad P_k de configuración del módulo de seguridad del chipset de seguridad de la tarjeta de chips 52. Este último incluye un submódulo de procesamiento 54_k destinado a aplicar a la clave de contenido CW la función $f^{-1}{}_k(y_k)$, inversa de la función $f_k(x_k)$, aplicada en la plataforma de codificación 2 que tiene por entrada el valor y_k suministrado por el chipset de seguridad de la tarjeta de chips 52.

Si el dato y_k suministrado por el chipset de seguridad de la tarjeta de chips 52 no corresponde al dato x_k utilizado a nivel de la plataforma de codificación, entrada de la función f_k, esto significará que la propiedad P_k configurada por el operador no se ha respetado. En este caso, el valor de la clave de contenido CW no se revela por el descifrado cooperado y la descodificación conduce a un resultado incomprensible en lo que sigue de la cadena de procesamiento del contenido, normalmente la descodificación.

En otra variante de la invención, el procedimiento se implementa para proteger la interfaz entre el chipset del descodificador 50 y el chipset de seguridad de la tarjeta del chips 52.

En este caso, el chipset de seguridad de la tarjeta de chips 52 incluye al menos un submódulo de sobre-cifrado 54_i, i = 1 a n, que comprende una rutina destinada a aplicar a la clave CW cifrada al menos una función f_i, que tiene por parámetros de entrada un dato x_i, representativo de una propiedad P_i de configuración de hardware y/o software de la interfaz entre el chipset del descodificador 50 y el chipset de seguridad de la tarjeta de chips 52.

La unidad de cálculo 40 del chipset del descodificador 50 incluye al menos un submódulo de procesamiento 42i, i = 1 a n, destinado a aplicar a la clave de contenido CW al menos una función $f^{-1}{}_i(y_i)$, i = n a 1, inversa de la función $f_i(x_i)$, i = 1 a n, aplicada en el chipset de seguridad de la tarjeta de chips 52.

Si el dato y_i suministrado por el chipset del descodificador 50 no corresponde al dato x_i utilizado por el submódulo de sobre-cifrado 54_i del chipset de seguridad de la tarjeta de chips 52, entrada de la función f_i, esto significará que la propiedad de hardware y/o software P_i de la interfaz entre el chipset del descodificador 50 y el chipset de seguridad de la tarjeta de chips 52 configurada por el operador no se ha respetado. En este caso, el valor de la clave de contenido CW no se descifra correctamente y la descodificación conduce a un resultado incomprensible en lo que sigue de la cadena de procesamiento del contenido, normalmente la descodificación.

La tabla que sigue describe, a título de ejemplo no limitativo, unas propiedades Pi internas en el entorno de seguridad o externas a este que pueden utilizarse por el procedimiento según la invención.

Propiedad	Objetivo del control de la propiedad	Interés
Valor representativo de las características actuales del entorno de seguridad del terminal, normalmente el módulo de seguridad del chipset	Conformidad de las características actuales del entorno de seguridad del terminal (conformidad con el mapa de fusión, funcionalidades activadas o desactivadas (JTAG bloqueado, boot loader en modo seguridad, indicador de primer lanzamiento efectuado (instalación del entorno del terminal objetivo), cifrado de la FLASH activa, cifrado de la RAM activa, ...), número de claves, ...)	Control de la conformidad del entorno de seguridad del terminal con relación a las exigencias y a la política de seguridad de control de las actualizaciones Anti-mosc
...		

Estado actual de las salidas A/V	Verificación de las salidas autorizadas para el contenido (HDMI, HDD, Ethernet, Wifi, ...)	Control E2E de la conformidad de la política de redistribución del contenido
Estado actual de los mecanismos de protección asociados a las salidas A/V	Activación de los mecanismos de protección del contenido en las salidas autorizadas (HDCP, Macrovison, DTCPIP, ...)	
...		
Valor representativo de los servicios autorizados y/o de los derechos de uso adquiridos por el agente de control de acceso	Conformidad de los servicios autorizados (lista de los identificadores de servicios o de los operadores asociados) y normalidad de los derechos de uso adquiridos (número de derechos, fecha de expiración de los derechos, ...)	Control de la conformidad del control de acceso realizada por el agente de control de las actualizaciones Anti MOSC
Valor representativo de las listas de revocaciones asociadas a unos mecanismos de protección de la salida A/V	Conformidad de la versión actual de las listas de revocaciones asociadas a unos mecanismos de protección de salidas A/V (HDCP, DTCP-IP, CI+, CPCM, ...)	
...		
Valor representativo de los parámetros actuales de acceso al (a los) servicio(s) del operador	Conformidad de los parámetros actuales de acceso al (a los) servicio(s) del operador (dirección del portal de servicios, ...)	Control de la conformidad del servicio proporcionado por el control de las actualizaciones
Valor representativo de la clave de protección del contenido anterior	Supresión del acceso aleatorio al contenido (forzar el consumo de una parte de un contenido, normalmente una publicidad, para acceder a la parte siguiente o al menos su inicio, ...)	
…		

El procedimiento según la invención se aplica tanto a las soluciones DRM (por Digital Rights Management) como a las soluciones CAS (por Control Access System) para unos servicios lineales (directo) o no (VoD,…) transmitidos en unidifusión, multidifusión o en emisión.

Obsérvese que ya no se requiere la autenticidad de las informaciones transmitidas para el control de las salidas A/V de un terminal. En efecto, si estas no se posicionan correctamente antes de la revelación de la clave de contenido, estas últimas no se descodificarán correctamente.

Obsérvese igualmente que en el contexto de los servicios unidifusión (VoD,..), si el identificador del usuario o del terminal que ha adquirido una licencia o un derecho sirve igualmente de revelador, entonces este identificador puede utilizarse como marca válida para un dispositivo de marca de agua.

El procedimiento según la invención se controla de manera dinámica bajo el control del operador de los servicios desde la plataforma de codificación 2. Las propiedades del servicio tenidas en cuenta y sus valores representativos esperados pueden evolucionar con el transcurso del tiempo según las necesidades de limitaciones y las evoluciones de las contribuciones de los terminales objetivo por el operador.

La ejecución del proceso es estrictamente la misma sobre el conjunto de los terminales que reciben un mismo contenido, tanto si los valores de los datos característicos obtenidos sean o no conforme a sus valores esperados. No hay verificación, ni por tanto pruebas intermedias, y solo el valor final de la clave de contenido obtenida, que permite o no descifrar correctamente el contenido, indica o no, que el conjunto de los datos característicos tenidos en cuenta están de acuerdo con los valores esperados.

Gracias al procedimiento según la invención, se incrementa la complejidad para un atacante de recuperar la clave de contenido. Esta complejidad no se basa únicamente en el conocimiento de la clave preestablecida en el entorno de seguridad del terminal, sino que depende igualmente de la configuración del hardware y software utilizado para la implementación del servicio suministrado.

En otra variante de implementación del procedimiento según la invención, una parte de los reveladores es dinámica y representativa de la evolución del servicio o de su adaptación con relación a un contenido dado. En esta variante, el acceso a la clave de contenido impone una situación de conformidad del terminal.

Por otro lado, la protección del contenido de extremo a extremo, la protección del agente de control de acceso o la protección del servicio del operador de manera general, pueden relacionarse con la protección de la clave de contenido.

REIVINDICACIONES

1. Procedimiento de protección de un contenido (6) codificado mediante una clave de contenido CW, siendo suministrado dicho contenido por un sistema de emisión a al menos un terminal de recepción (4), siendo realizado el suministro de contenido por dicho sistema de emisión por medio de un servicio configurado localmente a nivel de dicho terminal de recepción por un conjunto de propiedades Pi, i = 1 a N, conocidas del sistema de emisión, estando representadas cada una de dichas propiedades Pi por un dato x_i memorizado en dicho sistema de emisión y por un dato y_i obtenido por medición o por cálculo en el entorno del terminal de recepción (4) y accesible localmente para lectura por este terminal de recepción (4) en el mismo encabezado que una clave K de acceso al contenido, en la emisión, estando dicha clave de contenido CW sobre-cifrada mediante una función invertible de cifrado F por medio de la clave de acceso al contenido K y al menos una función invertible de sobre-cifrado $f_i(x_i)$ dependiente de al menos unas propiedades Pi, i = 1 a n, procedimiento **caracterizado por que**:

en la emisión, incluye las etapas que consisten en:

- definir un subconjunto EP no vacío de propiedades Pi a verificar, i = 1 a n, siendo realizada la verificación de las propiedades Pi, i = 1 a n, sistemáticamente o de manera puntual,
- sobre-cifrar dicha clave de contenido CW aplicando, según una secuencia ordenada de funciones sobre dicha clave de contenido CW la función invertible F y las funciones invertibles de sobre-cifrado $f_i(x_i)$ para cada propiedad Pi, i = 1 a n, de dicho subconjunto EP,
- transmitir dicha clave de contenido CW sobre-cifrada al terminal (4) con una lista de referencias que representan un subconjunto EP de propiedades P_i del servicio a verificar, correspondiente a los datos x_i, i = 1 a n, utilizados para calcular las funciones invertibles de sobre-cifrado $f_i(x_i)$, y a los datos y_i, i = 1 a n, a utilizar para el cálculo por el terminal de las funciones inversas de sobre-cifrado $f_i^{-1}(y_i)$,

y en la recepción,

- para cada propiedad Pi perteneciente a dicho subconjunto EP, leer el dato local y_i de dicho terminal que representa dicha propiedad Pi,
- revelar el valor CW' de dicha clave de contenido CW aplicando sobre la clave de contenido sobre-cifrada, según una secuencia inversa a dicha secuencia ordenada, la función inversa de cifrado F^{-1} y las funciones inversas de sobre-cifrado $f_i^{-1}(y_i)$ para cada una de las propiedades Pi de dicho subconjunto EP, no siendo revelada la clave de contenido más que después de la verificación de todas las propiedades P_i, i = 1 a n, de dicho subconjunto EP,
- descodificar el contenido por medio del valor revelado CW' de dicha clave de contenido CW.

2. Programa informático memorizado sobre un soporte de registro **caracterizado por que** incluye unas instrucciones para implementar las etapas del procedimiento según la reivindicación 1 implementadas en la emisión, cuando son ejecutadas por un ordenador.

3. Plataforma de codificación (2) de un contenido mediante una clave de contenido CW, siendo suministrado dicho contenido por dicha plataforma a al menos un terminal (4) de recepción por medio del servicio configurado localmente a nivel de dicho terminal de recepción según un conjunto de propiedades P_i, i = 1 a N, conocidas de dicha plataforma, estando representadas cada una de dichas propiedades a verificar Pi por un dato x_i memorizado en dicha plataforma y por un dato y_i obtenido por medición o por cálculo en el entorno del terminal de recepción (4) y accesible localmente para lectura por este terminal de recepción en el mismo encabezado que una clave K de acceso al contenido, plataforma de codificación que incluye:

- unos medios para definir un subconjunto EP no vacío de propiedades P_i a verificar, i = 1 a n, siendo realizada la verificación de las propiedades P_i sistemáticamente o de manera puntual,
- unos medios para sobre-cifrar dicha clave de contenido CW aplicando, según una secuencia ordenada de funciones, una función invertible de cifrado F por medio de la clave de acceso al contenido K y al menos una función invertible de sobre-cifrado $f_i(x_i)$ para cada propiedad P_i, i = 1 a n, subconjunto EP,
- unos medios para transmitir dicha clave de contenido CW sobre-cifrada al terminal (4) con una lista de referencias que representan un subconjunto EP de las propiedades P_i del servicio a verificar, correspondiente a los datos x_i, i = 1 a n, utilizados para calcular las funciones invertibles de sobre-cifrado $f_i(x_i)$, y a los datos y_i, i = 1 a n, a utilizar para el cálculo por el terminal (4) de las funciones inversas de sobre-cifrado $f_i^{-1}(y_i)$.

4. Plataforma de descodificación de un contenido codificado mediante una clave de contenido CW, siendo suministrado dicho contenido por una plataforma de codificación a la plataforma de descodificación por medio de un servicio configurado localmente a nivel de dicha plataforma de descodificación según un conjunto de propiedades a verificar P_i, i = 1 a n, conocidas por dicha plataforma de codificación, estando representadas cada una de dichas propiedades P_i por un dato x_i memorizado en dicha plataforma de codificación y por un dato y_i obtenido por medición o por cálculo en el entorno de la plataforma de descodificación y accesible localmente para lectura por esta plataforma de descodificación en el mismo encabezado que una clave K de acceso al contenido, siendo realizada la verificación de dichas propiedades Pi, i = 1 a n, sistemáticamente o de manera puntual,

plataforma de descodificación **caracterizada por que** incluye:

- unos medios para recibir la clave de contenido CW sobre-cifrada y una lista de referencias que representan un subconjunto EP no vacío de propiedades P_i a verificar, i = 1 a n, correspondiente a los datos x_i, i = 1 a n, utilizados por la plataforma de codificación para calcular unas funciones invertibles de sobre-cifrado $f_i(x_i)$, y a los datos y_i, i = 1 a n, a utilizar por la plataforma de descodificación para calcular unas funciones inversas de sobre-cifrado $f_i^{-1}(y_i)$, siendo sobre-cifrada la clave de contenido mediante aplicación sobre la clave de contenido CW, según una secuencia ordenada de funciones, de una función invertible de sobre-cifrado F por medio de la clave de acceso al contenido K y de al menos una función invertible de sobre-cifrado $f_i(x_i)$ para cada propiedad P_i, i = 1 a n, subconjunto EP,
- unos medios para leer el dato local y_i que representa cada propiedad Pi de dicho subconjunto EP,
- unos medios para revelar el valor CW' de dicha clave de contenido CW aplicando sobre la clave de contenido sobre-cifrada, según una secuencia inversa a dicha secuencia ordenada, la función inversa de cifrado F^{-1} y las funciones inversas de sobre-cifrado $f_i^{-1}(y_i)$ para cada una de las propiedades Pi de dicho subconjunto EP, no siendo revelada la clave de contenido más que después de la verificación de todas las propiedades P_i, i = 1 a n, del subconjunto EP,
- unos medios para descodificar el contenido por medio del valor revelado de dicha clave de contenido.

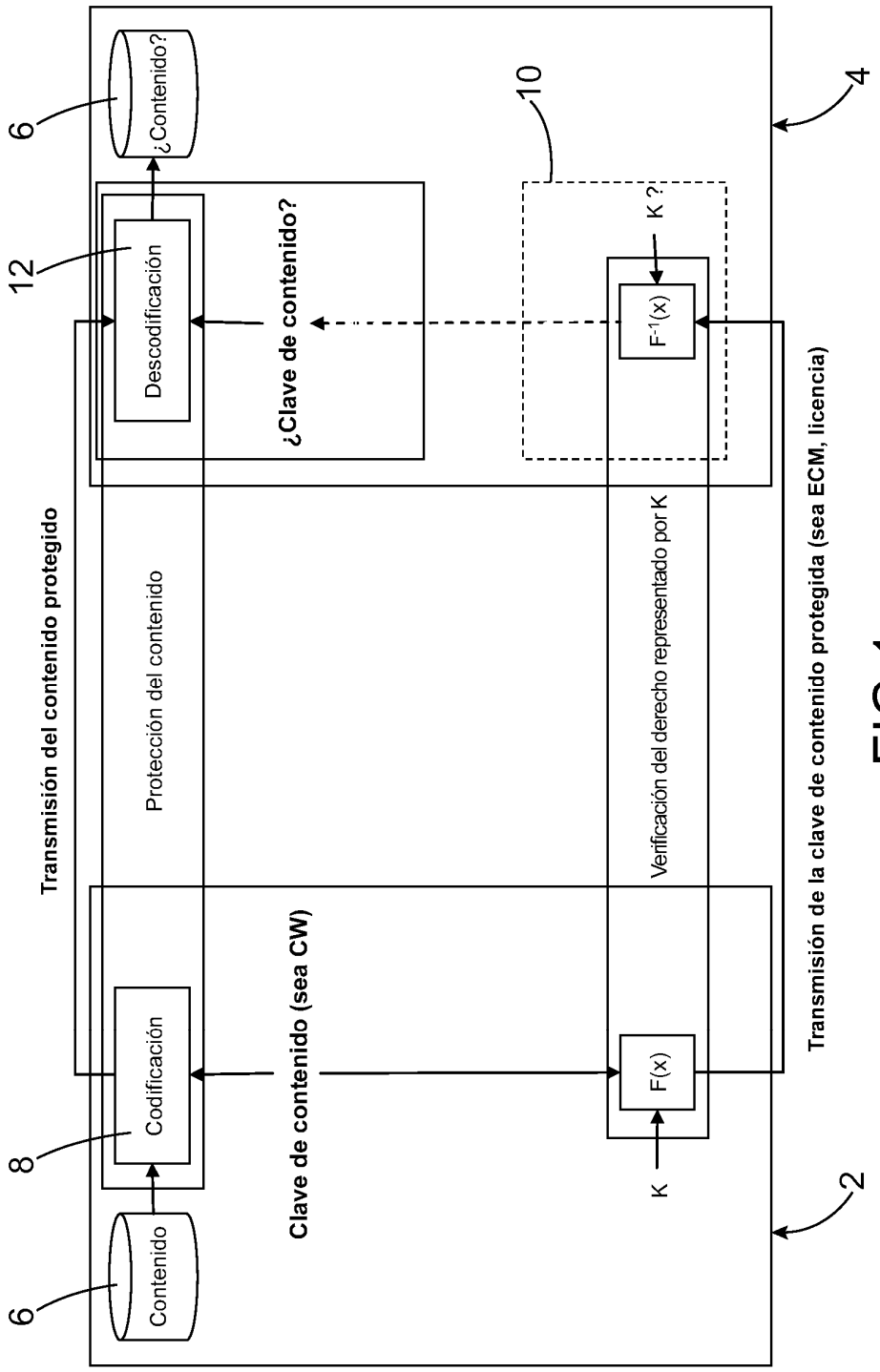
6
¿Contenido?
10
4
12
Descodificación
¿Clave de contenido?
K ?
F-1(x)
Transmisión del contenido protegido
Protección del contenido
Verificación del derecho representado por K
Transmisión de la clave de contenido protegida (sea ECM, licencia)
8
Codificación
Clave de contenido (sea CW)
F(x)
K
6
Contenido
2

FIG.1

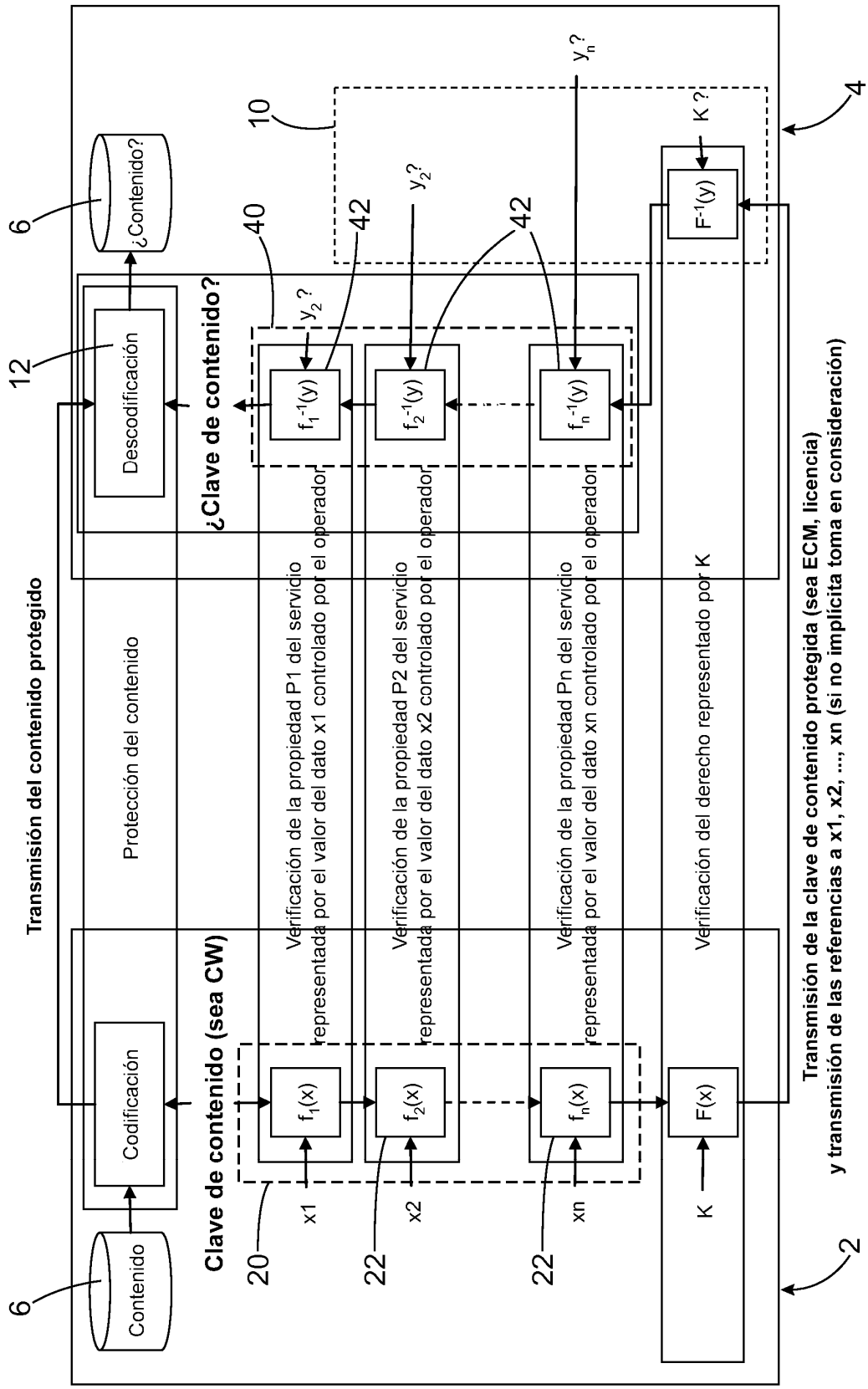
Transmisión del contenido protegido
Contenido
Codificación
Protección del contenido
Descodificación
¿Contenido?
Clave de contenido (sea CW)
¿Clave de contenido?
Verificación de la propiedad P1 del servidio representada por el valor del dato x1 controlado por el operador
Verificación de la propiedad P2 del servidio representada por el valor del dato x2 controlado por el operador
Verificación de la propiedad Pn del servidio representada por el valor del dato xn controlado por el operador
Verificación del derecho representado por K
Transmisión de la clave de contenido protegida (sea ECM, licencia)
y transmisión de las referencias a x1, x2, ..., xn (si no implícita toma en consideración)
f1(x)
f2(x)
fn(x)
F(x)
f1-1(y)
f2-1(y)
fn-1(y)
F-1(y)
x1
x2
xn
K
y2 ?
yn ?
K ?
2
4
6
6
10
12
20
22
22
40
42
42

FIG.2

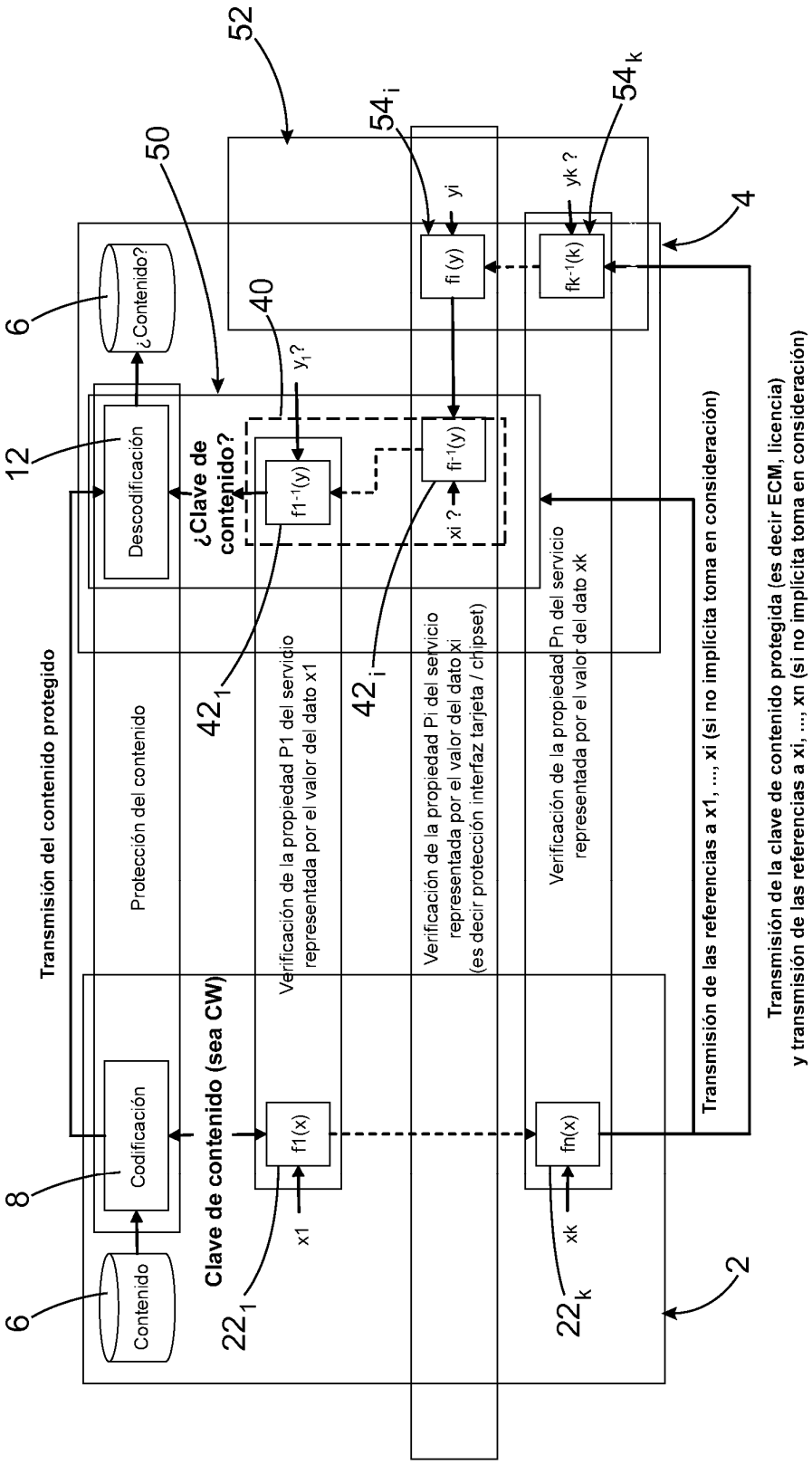
52
50
54i
54k
4
6
¿Contenido?
40
yi
yk ?
fi (y)
fk-1(k)
12
Descodificación
¿Clave de contenido?
y1?
f1-1(y)
fi-1(y)
xi ?
42i
421
Transmisión del contenido protegido
Protección del contenido
Verificación de la propiedad P1 del servicio representada por el valor del dato x1
Verificación de la propiedad Pi del servicio representada por el valor del dato xi (es decir protección interfaz tarjeta / chipset)
Verificación de la propiedad Pn del servicio representada por el valor del dato xk
Transmisión de las referencias a x1, ..., xi (si no implícita toma en consideración)
Transmisión de la clave de contenido protegida (es decir ECM, licencia) y transmisión de las referencias a xi, ..., xn (si no implícita toma en consideración)
8
Codificación
Clave de contenido (sea CW)
f1(x)
fn(x)
x1
xk
6
Contenido
221
22k
2

FIG.3