(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 562 053**

(51) Int. CI.:

G06F 21/10 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **06.10.2005 E 05787954 (6)**

(97) Fecha y número de publicación de la concesión europea: **23.12.2015 EP 1800200**

(54) Título: **Cifrado de claves de contenido basado en el usuario para un sistema de DRM**

(30) Prioridad:

08.10.2004 US 617189 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.03.2016

(73) Titular/es:

KONINKLIJKE PHILIPS N.V. (100.0%)
HIGH TECH CAMPUS 5
5656 AE EINDHOVEN, NL

(72) Inventor/es:

VAN LOENEN, ARNO KASPER;
VAN DEN HEUVEL, SEBASTIAAN ANTONIUS F.A.
y
ZWART, SJOERD

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Cifrado de claves de contenido basado en el usuario para un sistema de DRM

La presente invención se refiere en general a sistemas de Gestión de Derechos Digitales (DRM) para controlar contenido electrónico y más específicamente, se refiere a un sistema de DRM que utiliza cifrado de claves de contenido basado en el usuario.

La gestión de derechos digitales (DRM) es un enfoque sistemático para la protección de derechos de autor para medios digitales. El propósito de la DRM es impedir la distribución ilegal de contenido de pago. Algunos productos de DRM tempranos buscaban limitar la distribución ilegal del contenido vinculando el contenido a dispositivos específicos, de modo que el contenido solamente podía ser reproducido en un dispositivo autorizado. El problema con este enfoque es que un usuario puede tener varios dispositivos, situados dentro o cerca de su hogar, que podrían ser usados para reproducir el contenido (p. ej., un ordenador, un reproductor de DVD, un PDA, un automóvil, etc.). Según los dispositivos llegan a estar más interconectados dentro del hogar mediante enrutadores inalámbricos y otras tecnologías, vincular el contenido a un dispositivo específico llega a ser un inconveniente mayor.

Un reciente enfoque para abordar esta cuestión implica el concepto de un dominio autorizado. Un dominio autorizado es una red controlada dentro de la que el contenido puede ser usado libremente. El contenido sin embargo está restringido para cruzar la frontera del dominio. Por tanto, cada dispositivo dentro del dominio puede tener acceso al contenido en ese dominio, pero el intercambio de contenido fuera del dominio está delimitado por reglas estrictas.

Una de las cuestiones que deben ser abordadas para implementar dominios autorizados es cómo entregar contenido con seguridad al dominio de modo que los usuarios pertenecientes al dominio puedan acceder fácilmente al contenido, impidiendo a la vez que el contenido sea diseminado libremente fuera del dominio. Una solución es cifrar el contenido con una clave de contenido y luego proporcionar la clave de contenido a los dispositivo dentro del dominio. A fin de implementar una solución de ese tipo, se requiere un sistema para compartir con seguridad claves de contenido entre dispositivos en un dominio.

Se han propuesto varias soluciones. En un enfoque, se usa una sesión segura para intercambiar la clave de contenido cuando el intercambio tiene lugar entre un Emisor de Derechos y dispositivos del dominio o entre los mismos dispositivos. En este enfoque, la clave de contenido se almacena con seguridad en los dispositivos. Los inconvenientes de este sistema son que se requiere una sesión segura para intercambiar claves de contenido y el almacenamiento de claves de contenido necesita ser seguro.

En otro enfoque, la clave de contenido se cifra con una clave de usuario y solamente los dispositivos que tienen acceso a esta clave de usuario pueden descifrar la clave de contenido. Por ejemplo, en un sistema proporcionado por la OMA (Alianza Móvil Abierta), un Emisor de Derechos asigna una única clave de dominio para cada dominio y se permite a cada Emisor de Derechos asignar sus propias claves de dominio. No se requiere que las claves de dominio sean compartidas entre Emisores de Derechos. El resultado es que un dominio en general tendrá múltiples claves de dominio (es decir, cada dispositivo tiene una cantidad de claves de dominio igual al número de Emisores de Derechos cuyas licencias se usan). Un Emisor de Derechos cifrará una clave de contenido con la clave de dominio que ha asociado con el dominio que solicita la clave de contenido. Los dispositivos de un dominio pueden obtener las claves de dominio de los Emisores de Derechos para que puedan descifrar las claves de contenido.

En un sistema similar proporcionado por SMART-RIGHT™, el dominio tiene una clave de dominio y las claves de contenido son cifradas con esta clave de dominio. Los dispositivos del dominio intercambian con seguridad la clave de dominio y cada dispositivo retiene la clave de dominio.

Los inconvenientes de estos sistemas incluyen el hecho de que el contenido no puede desplazarse fácilmente a otro dominio, sin re-cifrar la clave de contenido o sin requerir algún otro proceso de trastienda en el Emisor de Derechos.

Se hace referencia al documento US 2003 / 0076955, con título “System and method for controlled copying and moving of content between devices and domains based on conditional encryption of content key depending on usage state”, que divulga la recepción de contenido en un dispositivo; el cifrado del contenido con una clave de contenido; el cifrado de la clave de contenido con una clave de dominio; y el almacenamiento de la clave de contenido cifrada y el contenido cifrado.

Se hace referencia al documento US 2004 / 0093523, con título “Group formation / management system, group management device, and member device” que divulga un sistema de formación / gestión de grupos, que comprende uno o más dispositivos miembros registrados operables para retener información secreta común única para un grupo.

En consecuencia, existe la necesidad de un sistema y procedimiento para distribuir con seguridad claves de contenido a dominios autorizados en un entorno de DRM.

La presente invención aborda los problemas citados anteriormente, así como otros, proporcionando un sistema y

procedimiento para utilizar el cifrado de claves de contenido basado en el usuario dentro de un dominio autorizado en un entorno de DRM. En un primer aspecto, la invención proporciona un sistema de gestión de derechos digitales (DRM) que tiene un dominio autorizado para gestionar medios digitales, en el que el dominio autorizado incluye una pluralidad de dispositivos interconectados que comprenden: un sistema de almacenamiento para almacenar una clave de usuario a partir de un usuario perteneciente al dominio autorizado; un sistema para descargar contenido cifrado con una clave de contenido; un sistema para descargar una clave de contenido cifrada; y un sistema de descifrado para descifrar la clave de contenido cifrada con la clave de usuario y para descifrar el contenido cifrado con la clave de contenido descifrada.

En un segundo aspecto, la invención proporciona un dispositivo de gestión de derechos digitales (DRM) para su uso en un dominio autorizado de DRM, en el que el dispositivo de DRM incluye: un sistema para compartir datos con otros dispositivos en el dominio autorizado de DRM; un sistema de almacenamiento para recibir una clave de usuario a partir de un usuario perteneciente al dominio autorizado; un sistema para recibir contenido cifrado con una clave de contenido; un sistema para recibir una clave de contenido cifrada; y un sistema de descifrado para descifrar la clave de contenido cifrada con la clave de usuario y para descifrar el contenido cifrado con la clave de contenido descifrada.

En un tercer aspecto, la invención proporciona un procedimiento para implementar un sistema de gestión de derechos digitales (DRM) que tiene un dominio autorizado para gestionar medios digitales entre un conjunto de usuarios y un conjunto de dispositivos interconectados, que comprende: proporcionar una clave de usuario a cada uno de los dispositivos en el dominio autorizado; cargar contenido desde un proveedor de contenido en uno de los dispositivos en el dominio autorizado, en el que el contenido está cifrado con una clave de contenido; proporcionar la clave de usuario a un emisor de derechos mediante un canal seguro; cargar una clave de contenido cifrado a partir del emisor de derechos en uno de los dispositivos en el dominio autorizado, en el que la clave de contenido está cifrada con la clave de usuario; descifrar la clave de contenido cifrada en uno de los dispositivos en el dominio autorizado con la clave de usuario; descifrar el contenido cifrado en uno de los dispositivos en el dominio autorizado con la clave de contenido descifrada; y usar el contenido descifrado en uno de los dispositivos en el dominio autorizado.

En un cuarto aspecto, la invención proporciona un sistema de gestión de derechos digitales (DRM) que tiene un dominio autorizado para gestionar medios digitales, en el que el dominio autorizado incluye una pluralidad de dispositivos interconectados que comprenden: un sistema de almacenamiento para almacenar una clave de usuario para cada usuario perteneciente al dominio autorizado; un sistema para descargar contenido cifrado con una clave de contenido; un sistema para descargar con seguridad una clave de contenido asociada a un usuario en el dominio autorizado; un sistema de cifrado para cifrar la clave de contenido con la clave de usuario del usuario asociado; y un sistema de descifrado para descifrar la clave de contenido cifrada con la clave de usuario del usuario asociado y para descifrar el contenido cifrado con la clave de contenido descifrada.

En un quinto aspecto, la invención proporciona un dispositivo de gestión de derechos digitales (DRM) para su uso en un dominio autorizado de DRM, en el que el dispositivo de DRM incluye: un sistema para compartir datos con otros dispositivos en el dominio autorizado de DRM; un sistema de almacenamiento para recibir una clave de usuario a partir de un usuario perteneciente al dominio autorizado; un sistema para recibir contenido cifrado con una clave de contenido; un sistema para recibir con seguridad una clave de contenido; un sistema para cifrar la clave de contenido con la clave de usuario asociada; y un sistema de descifrado para descifrar la clave de contenido cifrada con la clave de usuario y para descifrar el contenido cifrado con la clave de contenido descifrada.

En un sexto aspecto, la invención proporciona un procedimiento para implementar un sistema de gestión de derechos digitales (DRM) que tiene un dominio autorizado para gestionar medios digitales entre un conjunto de usuarios y un conjunto de dispositivos interconectados, que comprende: proporcionar una clave de usuario a cada uno de los dispositivos en el dominio autorizado; cargar contenido desde un proveedor de contenido en uno de los dispositivos en el dominio autorizado, en el que el contenido está cifrado con una clave de contenido; cargar una clave de contenido desde el emisor de derechos en uno de los dispositivos en el dominio autorizado mediante un canal seguro; cifrar la clave de contenido dentro de uno de los dispositivos en el dominio autorizado usando la clave de usuario asociada; descifrar la clave de contenido cifrada dentro de uno de los dispositivos en el dominio autorizado con la clave de usuario; descifrar el contenido cifrado dentro de uno de los dispositivos en el dominio autorizado con la clave de contenido descifrada; y usar el contenido descifrado en uno de los dispositivos en el dominio autorizado.

En un séptimo aspecto, la invención proporciona un sistema de gestión de derechos digitales (DRM) que tiene un dominio autorizado para gestionar medios digitales, en el que el dominio autorizado incluye una pluralidad de dispositivos interconectados que comprenden: un sistema para descargar y almacenar una clave de usuario mediante un canal seguro desde un emisor de derechos; un sistema para descargar contenido cifrado con una clave de contenido; un sistema para descargar una clave de contenido cifrada desde el emisor de derechos; y un sistema de descifrado para descifrar la clave de contenido cifrada con la clave de usuario asociada y para descifrar el contenido cifrado con la clave de contenido descifrada.

En un octavo aspecto, la invención proporciona un dispositivo de gestión de derechos digitales (DRM) para su uso en un dominio autorizado de DRM, en el que el dispositivo de DRM incluye: un sistema para compartir datos con otros

dispositivos en el dominio autorizado de DRM; un sistema para descargar y almacenar una clave de usuario a partir de un emisor de derechos mediante un canal seguro; un sistema para cargar con seguridad una clave de usuario en un

usuario; un sistema para recibir contenido cifrado con una clave de contenido; un sistema para recibir una clave de contenido cifrada con la clave de usuario; y un sistema de descifrado para descifrar la clave de contenido cifrada con la clave de usuario y para descifrar el contenido cifrado con la clave de contenido descifrada.

En un noveno aspecto, la invención proporciona un procedimiento para implementar un sistema de gestión de derechos digitales (DRM) que tiene un dominio autorizado para gestionar medios digitales entre un conjunto de usuarios y un conjunto de dispositivos interconectados que comprende: cargar una clave de usuario, desde un emisor de derechos en al menos un dispositivo en el dominio autorizado por un canal seguro; cargar la clave de usuario desde un emisor de derechos en una tarjeta inteligente perteneciente a un usuario; cargar contenido desde un proveedor de contenido en uno de los dispositivos en el dominio autorizado, en el que el contenido está cifrado con una clave de contenido; cargar una clave de contenido cifrada desde el emisor de derechos en uno de los dispositivos en el dominio autorizado, en el que la clave de contenido está cifrada con la clave de usuario; descifrar la clave de contenido cifrada en uno de los dispositivos en el dominio autorizado, con la clave de usuario; descifrar el contenido cifrado en uno de los dispositivos en el dominio autorizado con la clave de contenido descifrada; y usar el contenido descifrado en uno de los dispositivos en el dominio autorizado. De acuerdo con la invención, se proporcionan un dispositivo de sistemas de gestión de derechos digitales según lo definido en la reivindicación 1, un procedimiento según lo definido en la reivindicación 8 y un programa de ordenador según lo definido en la reivindicación 11.

Estas y otras características de esta invención serán entendidas más fácilmente a partir de la siguiente descripción detallada de los diversos aspectos de la invención considerada conjuntamente con los dibujos adjuntos, en los que:

La Figura 1 ilustra un sistema de DRM que tiene un dominio autorizado.

La Figura 2 ilustra un sistema de DRM que tiene un dominio autorizado que utiliza el cifrado de claves de contenido basado en usuario de acuerdo con una primera realización de la presente invención.

La Figura 3 ilustra un sistema de DRM que tiene un dominio autorizado que utiliza el cifrado de claves de contenido basado en usuario de acuerdo con una segunda realización de la presente invención.

La Figura 4 ilustra un sistema de DRM que tiene un dominio autorizado que utiliza el cifrado de claves de contenido basado en usuario de acuerdo con una tercera realización de la presente invención.

Con referencia ahora a los dibujos, la Figura 1 ilustra un panorama general de un sistema de DRM 10. El sistema de DRM 10 incluye un dominio autorizado 12, un emisor de derechos 18 y un proveedor de contenido 20. Un dominio autorizado 12 por ejemplo puede comprender un entorno hogareño que incluye un conjunto de usuarios 14 (p. ej., el Usuario 14A, el Usuario 14B) y un conjunto de dispositivos interconectados 16 (p. ej., 16A, 16B, 16C). En general, los dispositivos 16 están interconectados por cualquier tipo de red tal como una red de área local, una red privada virtual, Internet, una intranet, una red inalámbrica, etc. Los usuarios 14 pueden estar representados por tarjetas inteligentes u otros dispositivos y sistemas que puedan autentificar al usuario y los dispositivos 16 comprenden dispositivos habilitados para DRM que pueden representar (es decir, usar, reproducir, exhibir, etc.) contenido protegido por DRM. Un emisor de derechos 18 se refiere en general a un tercero fiable tal como los conocidos en la técnica. Sin embargo, las funciones proporcionadas por el emisor de derechos 18 pueden ser efectuadas por el proveedor de contenido 20. En funcionamiento, un usuario toma contacto con el proveedor de contenido 20 para obtener el contenido protegido por DRM C 13. Los derechos de uso R 11, tales como una licencia para el contenido son obtenidos de un emisor de derechos 18. Una vez que el contenido C 13 y los derechos R 11 son entregados al dominio autorizado 12, el usuario puede utilizar cualquiera de los dispositivos (16A, 16B, 16C) para representar el contenido. Según se describe más adelante, el contenido está cifrado con una clave de contenido y la clave de contenido está cifrada con una “clave de usuario”, p. ej., (1) una clave pública de un par de claves de usuario pública / privada según lo utilizado en el cifrado asimétrico de claves, tal como una infraestructura de clave pública (PKI), (2) una clave simétrica, etc. Para los fines del cifrado asimétrico de claves, la “clave de usuario” se refiere a la clave pública para los fines de cifrado y a la clave privada para los fines de descifrado.

La presente invención proporciona diversas realizaciones para implementar el cifrado de claves de contenido basado en el usuario. La Figura 2 ilustra una primera realización ilustrativa para implementar la invención que utiliza el cifrado de claves de contenido basado en el usuario. En esta realización, a un usuario (p. ej., el Usuario A) que se incorpora al dominio 12 se le proporciona una clave de usuario KA 19, p. ej., incrustada en una tarjeta inteligente, que se proporciona a todos los dispositivos 16 en el dominio 12 (en el caso de cifrado asimétrico, por ejemplo, solamente la clave privada tendría que ser intercambiada). La clave de usuario puede ser intercambiada de manera segura. A un emisor de derechos 18 también se le proporciona la clave de usuario KA 19 para cifrar una clave de contenido CK 15, que fue obtenida desde el proveedor de contenido 20. Cuando el usuario adquiere una licencia, un conjunto de derechos 30 que comprende la licencia 26 y la clave de contenido cifrada 34 se envía a un dispositivo en el dominio 12. Una vez que cualquiera de los dispositivos 16 recibe la clave de contenido cifrada 34, la clave puede ser descifrada con la clave de usuario KA 19 por un sistema de descifrado 28. La clave de contenido descifrada CK 15 puede luego ser usada para descifrar el contenido cifrado 32 proporcionado por el proveedor de contenido 20.

Un proceso ilustrativo se describe de la siguiente manera:

1. El Usuario A se incorpora al dominio 12. La tarjeta inteligente del Usuario A y los dispositivos 16 en el dominio 12 intercambiarán con seguridad la clave de usuario KA 19 asociada al Usuario A. Después del intercambio, cada dispositivo 16 retendrá la KA 19. Un nuevo dispositivo que se incorpore al dominio 12 será informado por otros dispositivos de la KA 19, o por el mismo dispositivo de usuario (p. ej., tarjeta inteligente) 14.

2. El Usuario A explora y adquiere un elemento de contenido de DRM C en un proveedor de contenido 20.

3. El Usuario A explora y adquiere una licencia en un emisor de derechos 18 para el elemento de contenido C.

4. La clave de contenido CK 15 (la clave usada para cifrar el elemento de contenido C) es intercambiada con seguridad por un proceso de trastienda entre el proveedor de contenido 20 y el emisor de derechos 18.

5. El Usuario A envía con seguridad su clave de usuario KA 19 al emisor de derechos 18. Optativamente, el emisor de derechos 18 almacena en memoria caché la clave de usuario KA 19 para su uso futuro.

6. El emisor de derechos 18 cifra la clave de contenido CD 15 como $CK_{cifrada, KA}$, con la clave de usuario KA 19. $CK_{cifrada, KA}$ = Cifrar (CK, KA).

7. La clave de contenido cifrada $CK_{cifrada, KA}$ se entrega a un dispositivo en el dominio 12 del Usuario A. Además, la licencia se entrega a un dispositivo del dominio del Usuario A. La $CK_{cifrada, KA}$ puede ser incrustada en la licencia o puede ser enviada por separado.

8. El elemento de contenido C 13 es cifrado con la clave de contenido CK 15. $C_{cifrado}$ = Cifrar (C, CK) y es entregado a un dispositivo en el dominio 12 del Usuario A.

9. Un usuario del dominio usa un dispositivo para representar el elemento de contenido cifrado C 13. Después de que la licencia ha concedido permiso para usar el elemento de contenido C, el dispositivo descifra la clave de contenido cifrada $CK_{cifrada, KA}$, usando la KA 19, dando como resultado CK 15. CK = Descifrar ($CK_{cifrada, KA}$, KA). El dispositivo usa luego la clave de contenido descifrada CK 15 para descifrar el elemento de contenido $C_{cifrado}$ 32. C = Descifrar ($C_{cifrado}$, CK), después de lo que el dispositivo puede usar el elemento de contenido C 13 (reproducir, representar, etc.).

Un escenario similar es posible para el Usuario B, reemplazando el Usuario A por B y reemplazando KA por KB. Dado que cada dispositivo en el dominio 12 retiene ambas claves de usuario de los Usuarios A y B, cada dispositivo es capaz de usar el contenido de ambos usuarios.

Una segunda realización de un sistema de cifrado claves de contenido basado en el usuario está ilustrada en la Figura 3. En esta realización, cada usuario (Usuario A, Usuario B) tiene una clave (p. ej., KA 19 para el Usuario A y KB 21 para el Usuario B), pero el emisor, o emisores, de derechos 18 no sabe(n) de las claves de usuario. Las claves de usuario son conocidas solamente con el dominio 12. El emisor de derechos 18 por lo tanto no cifra la clave de contenido CK 15 con una clave de usuario durante la entrega, sino que en cambio emite un conjunto de derechos 30 que comprenden una licencia 26 y una clave de contenido no cifrada CK 15 (ya sea por separado o en combinación), donde, como mínimo, la clave de contenido no cifrada es intercambiada mediante un canal seguro. El dispositivo receptor 16C comprueba la información de usuario 22 que está ligada a la licencia. Obsérvese que el emisor de derechos puede obtener la información de usuario 22 desde el proveedor de contenido 20 con la clave de contenido CK 15, o directamente desde el usuario cuando el usuario adquiere la licencia 26 a partir del emisor de derechos 18.

El dispositivo receptor usa un sistema de cifrado 24 para cifrar la clave de contenido CK 15 con la correspondiente clave de usuario KA 19, para generar una clave de contenido cifrada 34. La clave de usuario KA 19 se pone a disposición de todos los dispositivos 16 en el dominio 12 del usuario de modo que cada dispositivo pueda descifrar la clave de contenido cifrada 34 con un sistema de descifrado 28. Una vez que la clave de contenido CK está descifrada, el dispositivo puede descifrar el contenido cifrado y representar (es decir, reproducir, registrar, exhibir, etc.) el contenido C 13.

Una tercera realización de un sistema de cifrado de claves de contenido basado en el usuario se ilustra en la Figura 4. En esta realización, cuando el usuario (p. ej., el Usuario A) adquiere una licencia, el emisor de derechos 18 cifra la clave de contenido CK usando una clave de usuario KA 19 asignada por el emisor de derechos 18. El emisor de derechos 18 emite luego un conjunto de derechos 30 que comprende una licencia 26 y la clave de contenido cifrada 34 (ya sea por separado o en combinación). El emisor de derechos 18 también transmite con seguridad la clave de usuario KA 19 por un canal seguro 36 bien al usuario o bien a un dispositivo en el dominio 12. La clave de usuario KA 19 se deja luego a disposición para todos los dispositivos 16 en el dominio 12 de modo que cada dispositivo pueda descifrar la clave de contenido cifrada 34 con un sistema de descifrado 28.

Por tanto, en esta tercera realización, el emisor de derechos 18 asigna las claves de usuario a los usuarios. Debido a esto, un usuario puede tener múltiples claves de usuario generadas a partir de distintos emisores de derechos. Cuando un usuario adquiere licencias adicionales en el futuro, los Emisores de Derechos pueden reutilizar la clave de usuario asociada a este usuario.

Se entiende que los sistemas, funciones, mecanismos, procedimientos, motores y módulos descritos en la presente memoria pueden ser implementados en hardware, software o una combinación de hardware y software. Pueden ser implementados por cualquier tipo de sistema de ordenador u otro aparato adaptado para llevar a cabo los procedimientos descritos en la presente memoria. Una combinación habitual de hardware y software podría ser un sistema de ordenador de propósito general con un programa de ordenador que, cuando es cargado y ejecutado, controla el sistema de ordenador de modo que lleve a cabo los procedimientos descritos en la presente memoria. Alternativamente, podría utilizarse un ordenador de uso específico, que contenga hardware especializado para llevar a cabo una o más de las tareas funcionales de la invención. En una realización adicional, parte de o toda la invención podría ser implementada de forma distribuida, p. ej., por una red tal como Internet. Además, la invención podría ser proporcionada como un procedimiento de negocios o como un servicio por un proveedor de servicios sobre una red.

La presente invención también puede ser incrustada en un producto de programa de ordenador, que comprenda todas las características que permiten la implementación de los procedimientos y funciones descritos en la presente memoria y que – cuando se carga en un sistema de ordenador – es capaz de llevar a cabo estos procedimientos y funciones. Términos tales como programa de ordenador, programa de software, programa, producto de programa, software, etc., en el presente contexto significan cualquier expresión, en cualquier lenguaje, código o notación, de un conjunto de instrucciones planeadas para provocar que un sistema que tenga una capacidad de procesamiento de información realice una función específica ya sea directamente o después de una cualquiera o ambas de las siguientes: (a) conversión a otro lenguaje, código o notación; y / o (b) reproducción en una forma material distinta.

La descripción precedente de la invención ha sido presentada con fines de ilustración y descripción. No está concebida para ser exhaustiva o para limitar la invención a la forma exacta divulgada y obviamente, son posibles muchas modificaciones y variaciones. Tales modificaciones y variaciones, que pueden ser evidentes para una persona experta en la técnica se planea que estén incluidas dentro del ámbito de esta invención según lo definido por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un dispositivo de gestión de derechos digitales (DRM) (16A, 16B, 16C) incluido en un dominio autorizado de DRM (12), en el que el dispositivo de DRM incluye:

un sistema para compartir datos con otros dispositivos en el dominio autorizado de DRM;

un sistema de almacenamiento para recibir una clave de usuario (19) desde un usuario (14A, 14B) cuando el usuario se incorpora al dominio autorizado, estando el dispositivo configurado para intercambiar la clave de usuario con los dispositivos (16) en el dominio y para almacenar una clave de usuario a partir de cada uno de una pluralidad de usuarios pertenecientes al dominio autorizado;

un sistema para recibir contenido (13) cifrado con una clave de contenido (32);

un sistema para recibir una clave de contenido cifrado (34); y

un sistema de descifrado (28) para descifrar la clave de contenido cifrada con la clave de usuario y para descifrar el contenido cifrado con la clave de contenido descifrada.

2. El dispositivo de DRM de la reivindicación 1, en el que la clave de usuario está incrustada en una tarjeta inteligente.

3. El dispositivo de DRM de la reivindicación 1, en el que el contenido se descarga desde un proveedor de contenido (20).

4. El dispositivo de DRM de la reivindicación 1, en el que la clave de contenido cifrada se descarga desde un emisor de derechos (18).

5. El dispositivo de DRM de la reivindicación 1, en el que la clave de contenido cifrada se descarga con una licencia (26) que gobierna los derechos de uso del contenido descargado.

6. Un sistema de gestión de derechos digitales (DRM) que tiene un dominio autorizado (12) para gestionar medios digitales, en el que el dominio autorizado incluye una pluralidad de dispositivos interconectados (16) como en la reivindicación 1.

7. Un sistema de gestión de derechos digitales (DRM) como en la reivindicación 6, que comprende un conjunto de dispositivos (14) que representan usuarios, los dispositivos (14) que representan usuarios están configurados para intercambiar una clave de usuario (19) asociada al usuario, con la pluralidad de dispositivos de gestión de derechos digitales (16), cuando el usuario se incorpora al dominio.

8. Un procedimiento para implementar un sistema de gestión de derechos digitales (DRM) que tiene un dominio autorizado (12) para gestionar medios digitales entre un conjunto de usuarios y un conjunto de dispositivos interconectados (16), que comprende:

proporcionar una clave de usuario a partir de cada uno de una pluralidad de usuarios pertenecientes al dominio autorizado a cada uno de los dispositivos en el dominio autorizado;

cargar contenido (13) desde un proveedor de contenido a uno de los dispositivos en el dominio autorizado, en el que el contenido está cifrado con una clave de contenido (32);

proporcionar la clave de usuario a un emisor de derechos (18) mediante un canal seguro;

cargar una clave de contenido cifrada (34) desde el emisor de derechos a uno de los dispositivos en el dominio autorizado, en el que la clave de contenido está cifrada con la clave de usuario;

descifrar la clave de contenido cifrada en uno de los dispositivos en el dominio autorizado con la clave de usuario;

descifrar el contenido cifrado en uno de los dispositivos en el dominio autorizado con la clave de contenido descifrada; y

usar el contenido descifrado en uno de los dispositivos en el dominio autorizado.

9. El procedimiento de la reivindicación 8, en el que la clave de usuario se proporciona a cada uno de los dispositivos por un sistema seleccionado a partir del grupo que consiste en: una tarjeta inteligente y un dispositivo perteneciente al dominio autorizado.

10. El procedimiento de la reivindicación 8, en el que la etapa de cargar una clave de contenido cifrada desde el emisor de derechos incluye cargar una licencia.

11. Un programa de ordenador que, cuando se carga y ejecuta, controla un sistema de ordenador de modo que lleve a cabo uno cualquiera de los procedimientos 8 a 10.

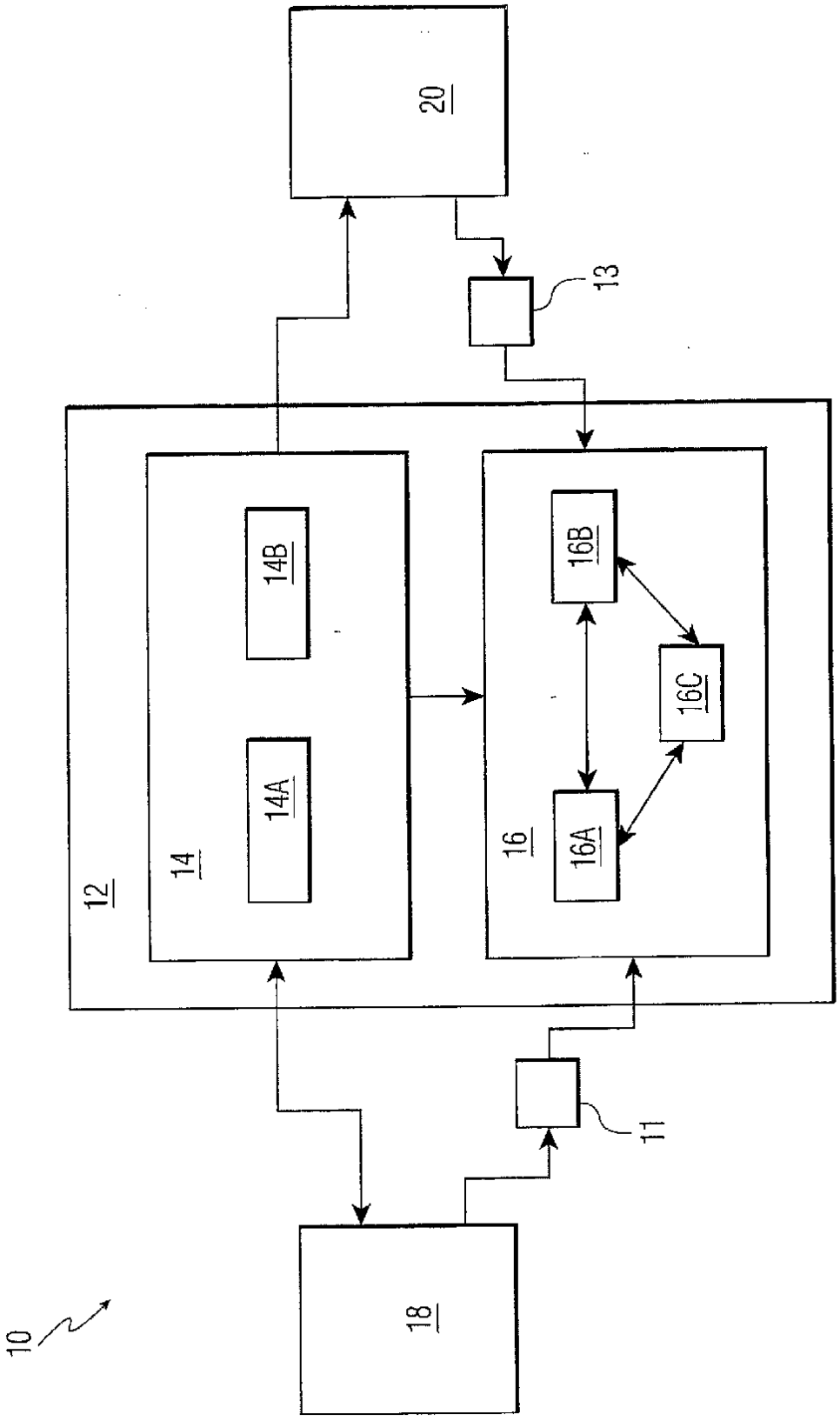

FIG. 1

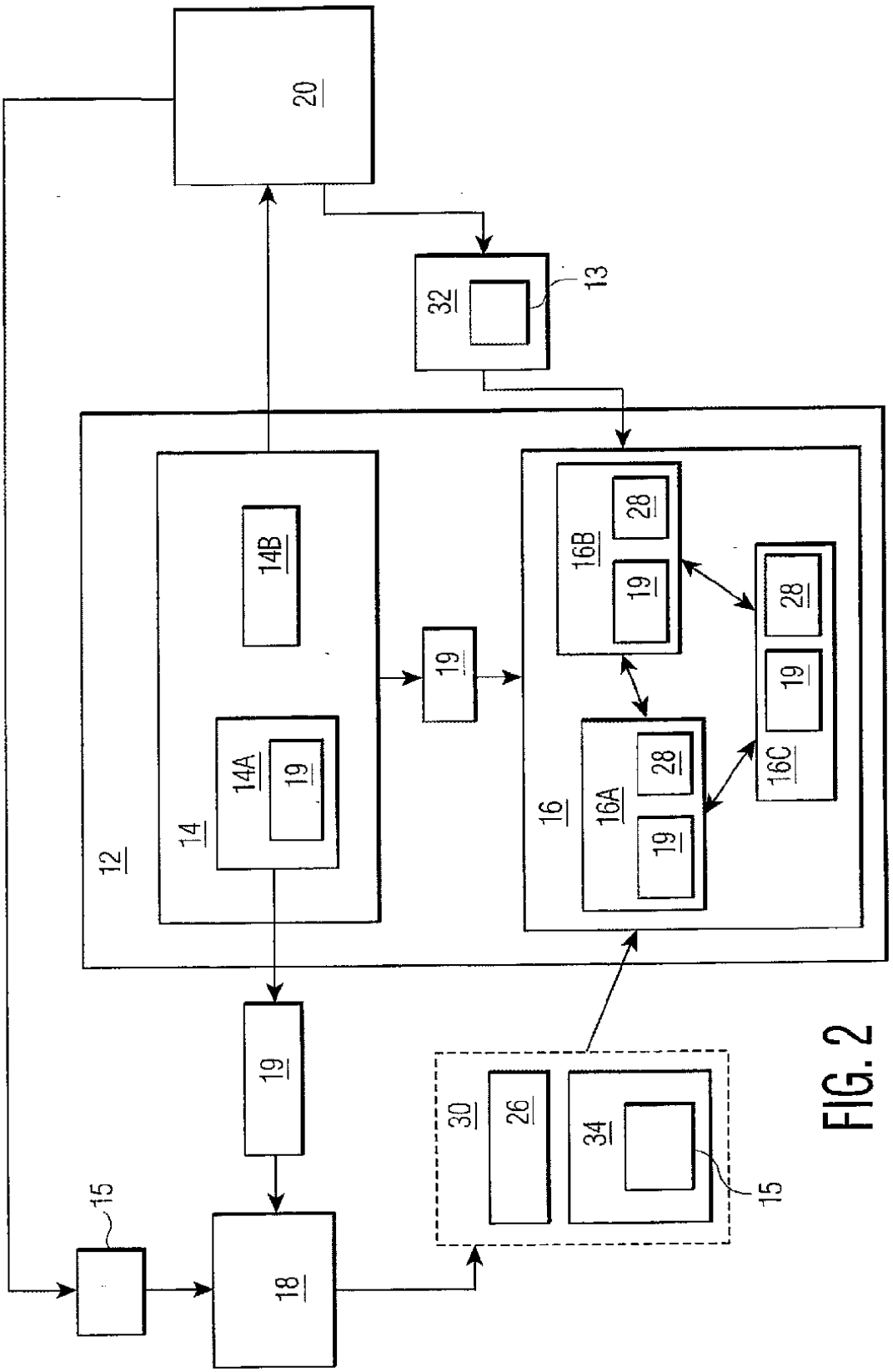
20
32
13
12
14
14B
14A
19
19
16
16B
28
19
28
19
16C
16A
28
19
19
30
26
34
15
15
18

FIG. 2

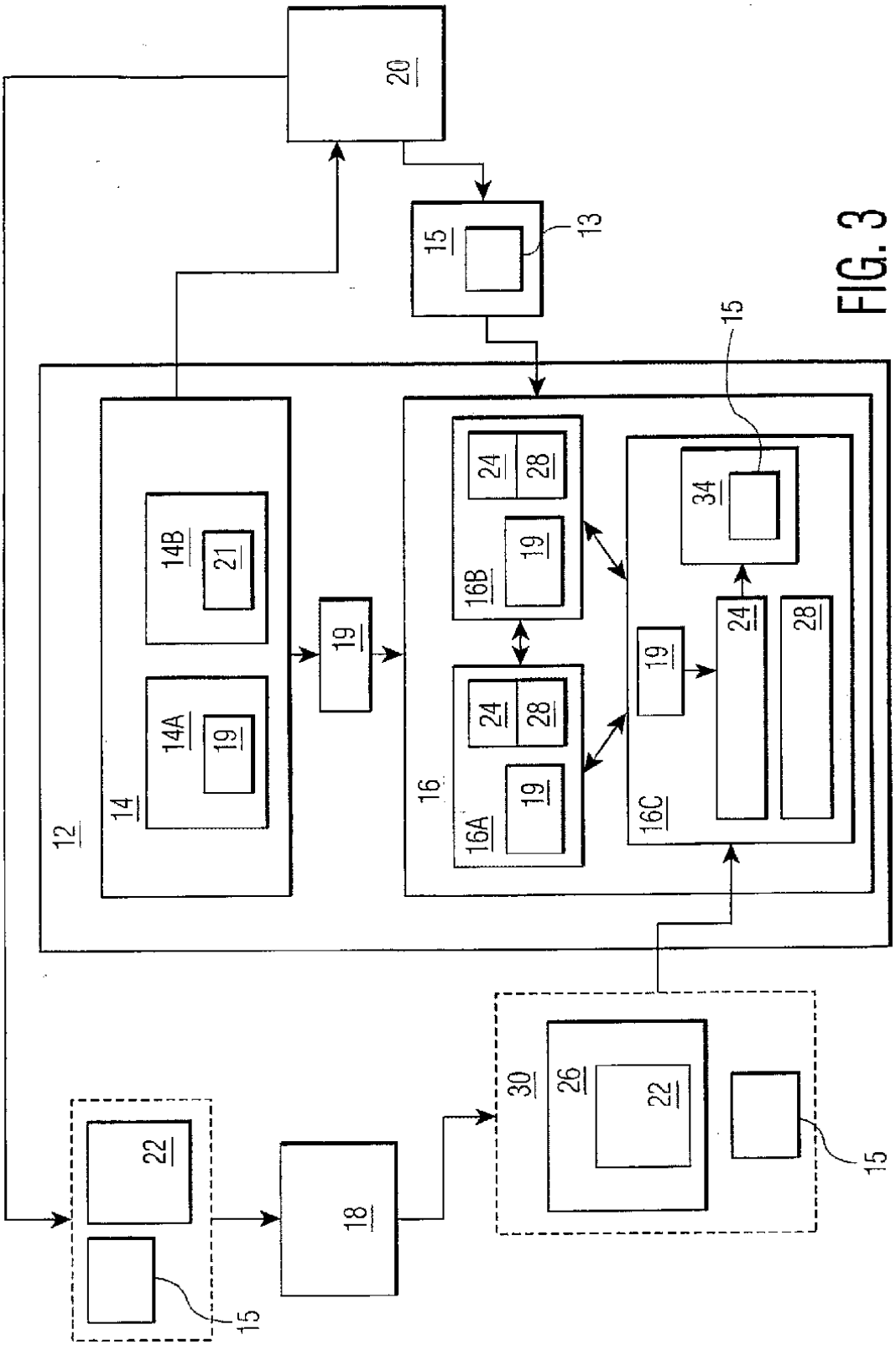
20
15
13
12
14
14B
21
14A
19
19
16
16B
24
28
19
16A
24
28
19
15
34
16C
19
24
28
18
22
15
30
26
22
15

FIG. 3

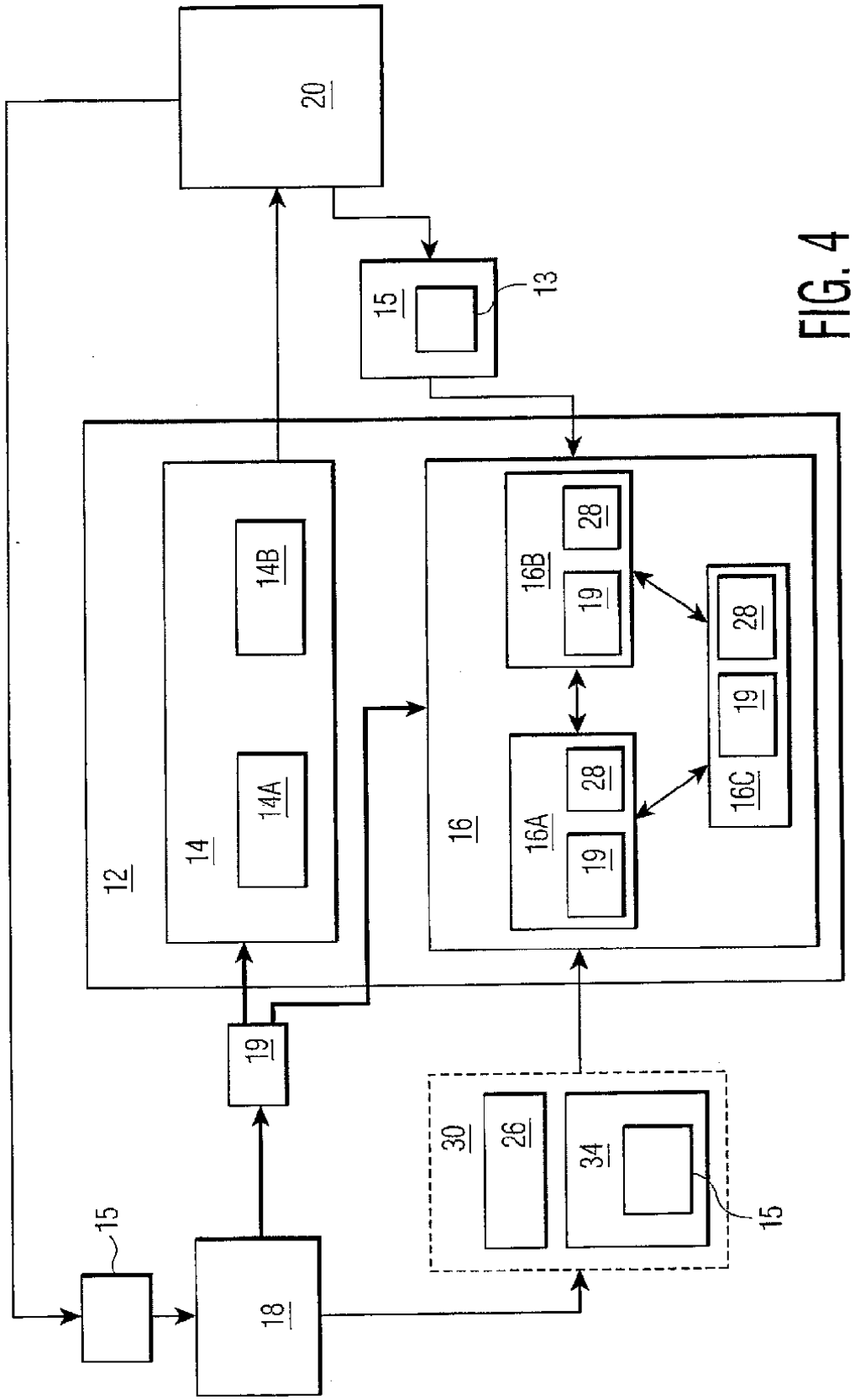

FIG. 4