(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 447 440**

(51) Int. CI.:

G06F 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **01.02.1996 E 05020699 (4)**

(97) Fecha y número de publicación de la concesión europea: **11.12.2013 EP 1643338**

(54) Título: **Un procedimiento y un sistema para gestionar un objeto de datos para cumplir con condiciones de uso predeterminadas**

(30) Prioridad:

01.02.1995 SE 9500355

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.03.2014

(73) Titular/es:

ROVI SOLUTIONS CORPORATION (100.0%)
2830 De La Cruz Boulevard
Santa Clara, CA 95050, US

(72) Inventor/es:

BENSON, GREG;
URICH, GREGORY H. y
KNAUFT, CHRISTOPHER

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Un procedimiento y un sistema para gestionar un objeto de datos para cumplir con condiciones de uso predeterminadas

La presente invención se refiere a un procedimiento y a un sistema para controlar el uso de un objeto de datos para cumplir unas condiciones de control de uso.

Una visión típica de la autopista de datos tiene redes regionales interconectadas con portadoras de datos a alta velocidad y larga distancia que proporcionan servicios de telecomunicaciones y una amplia gama de servicios interactivos en línea para los consumidores. A pesar de que la autopista de datos se encuentra en construcción, en la actualidad está abierta a un tráfico limitado.

El alcance de la información disponible para los consumidores se convertirá en verdaderamente global conforme se reduzcan drásticamente las barreras tradicionales a la entrada a la distribución de información y al acceso a la información. Esto significa que se dispondrá de información más diversa y especializada de manera tan conveniente como solían ser las fuentes genéricas de los principales proveedores.

Sin embargo, una autopista de datos totalmente operativa sólo será tan valiosa como los servicios reales que proporcione. Los servicios previstos para la autopista de datos que implican el suministro de objetos de datos (por ejemplo, libros, películas, vídeos, noticias, música, software, juegos, etc.) estarán y actualmente están limitados por la disponibilidad de dichos objetos. Antes de que los propietarios permitan que sus objetos de datos sean ofrecidos, deben garantizárseles los pagos por royalties y protección contra la piratería.

El cifrado es un componente clave de cualquier solución para proporcionar una protección contra copia. Pero cifrado, por sí solo, no es suficiente. Durante la transmisión y el almacenamiento, los objetos de datos estarán protegidos por el cifrado, pero en cuanto se proporciona la clave a alguien para descifrar el contenido, esa persona tendrá un control ilimitado sobre los objetos de datos. Debido a que el dominio digital permite que los objetos de datos sean reproducidos en cantidades ilimitadas, sin pérdida de calidad, cada objeto deberá ser protegido contra el uso ilimitado y la reproducción y la reventa no autorizadas.

El problema de protección no debe ser resuelto mediante una solución independiente para cada formato de datos particular. Sin embargo, si debiera haber algún tipo de estandarización, el estándar debería proporcionar adaptabilidad universal a las necesidades tanto de los proveedores como de los usuarios de datos.

El propietario del objeto de datos puede desear tener un control seguro permanente sobre cómo, cuándo, dónde y por quién es usada su propiedad. Además, puede desear definir diferentes reglas de compromiso para diferentes tipos de usuario y diferentes tipos de seguridad dependiendo del valor de los objetos particulares.

El usuario desea poder buscar y adquirir objetos de datos de una manera conveniente. El usuario debería ser capaz de combinar o editar los objetos adquiridos (es decir, para crear una presentación). Además, el usuario puede desear proteger a sus hijos de un material inapropiado.

Lo que se necesita es un sistema universalmente adaptable y un procedimiento para gestionar el intercambio y el uso de objetos de datos que, al mismo tiempo, proteja los intereses de los propietarios y de los usuarios de los objetos de datos.

El documento EP-A-0567800 describe un procedimiento para hacer cumplir el pago de royalties al copiar libros. Este procedimiento protege una secuencia de texto formateada de un documento estructurado que incluye un elemento de pago de royalties que tiene una etiqueta especial. Sin embargo, este procedimiento solo puede ser aplicado a documentos estructurados.

El documento EP-A-0715246 y las solicitudes relacionadas, EP-A-0715243, EP-A-0715244, EP-A-0715245 y EP-A-0715247 describen un sistema para controlar el uso y la distribución de obras digitales. Un creador crea una obra digital y, a continuación, determina los derechos de uso y los cánones apropiados. Estos derechos de uso, que definen la manera en la que puede usarse la obra digital, se adjuntan a la obra digital. El acceso a las obras digitales es controlado por repositorios seguros. La obra digital se almacena, con sus derechos de uso adjuntos, en un primer repositorio. Puede ser transmitida a un segundo repositorio si se establece que el segundo repositorio es confiable. La comunicación de una obra digital entre repositorios se realiza por medio de un canal de comunicación seguro.

Un objeto de la presente invención es proporcionar un procedimiento y un sistema para controlar el uso de un objeto de datos que sea independiente del formato de los objetos de datos y que proporcione seguridad de una manera flexible.

Según un primer aspecto de la presente invención, se proporciona un procedimiento para controlar el uso de un objeto de datos con el fin de cumplir las condiciones de control para el uso del objeto de datos, en el que el objeto de datos está contenido dentro de un paquete de datos que comprende dicho objeto de datos y un conjunto de datos de control, en el que dicho conjunto de datos de control comprende al menos un elemento de control de uso que define un uso del objeto de datos que cumple con las condiciones de control para el uso de un objeto de datos, en el que dicho conjunto de datos de control ha sido adaptado a un usuario específico y comprende al menos un identificador de datos de control, que identifica de manera única este conjunto de datos de control de usuario, y en el que el paquete de datos es seguro ya que el objeto de datos y los elementos de control de uso del conjunto de datos de control de usuario han sido cifrados, en el que el procedimiento comprende:

comprobar, en respuesta a una solicitud por parte de un usuario para usar el objeto de datos, si el uso solicitado cumple o no con el uso definido por el al menos un elemento de control de uso del conjunto de datos de control de usuario, y

en respuesta a si el uso solicitado cumple o no con el uso definido por el al menos un elemento de control de uso del conjunto de datos de control de usuario, descifrar el objeto de datos y permitir el uso solicitado,

en el que las etapas de comprobación, descifrado y concesión de permiso son realizadas por un programa de usuario almacenado por un procesador de datos del usuario,

y en el que el programa de usuario no permitirá ningún uso del objeto de datos cuando el uso solicitado no cumpla con dicho uso definido.

En realizaciones de la invención, los usos del objeto de datos, definidos por los elementos de control de uso, pueden estar definidos por el propietario del objeto de datos, por un intermediario, o por cualquier otra persona. Pueden diferir entre diferentes objetos. El control de uso es también independiente del formato del objeto de datos.

En una realización, los usos del objeto de datos definido por el uno o más elementos de control de uso comprenden uno o más de entre: el tipo de usuario, un límite de tiempo para el uso, un área geográfica para el uso, operaciones permitidas, el número de usos autorizados, el precio y la redistribución.

Las operaciones permitidas pueden incluir uno o más de entre: el visionado del objeto de datos, el uso del objeto de datos, la impresión del objeto de datos y la copia del objeto de datos.

Preferiblemente, los usos del objeto de datos comprenden una indicación del número de veces que el usuario está autorizado a usar el objeto de datos según al menos un elemento de control de usuario, y el procedimiento comprende, además, permitir solo el uso solicitado del objeto de datos cuando dicho número de veces es uno o más, y decrementar el número de veces en una unidad cuando se ha permitido el uso solicitado.

En una realización, el elemento de control de uso es actualizado después del uso del objeto de datos.

Preferiblemente, el programa de usuario nunca almacena el objeto de datos en formato nativo en el almacenamiento accesible por el usuario, y el procedimiento comprende además volver a empaquetar el objeto de datos en el paquete de datos seguro después del uso.

La presente invención se extiende también a un sistema para controlar el uso de un objeto de datos con el fin de cumplir con las condiciones de control para el uso del objeto de datos, en el que el objeto de datos está contenido dentro de un paquete de datos que comprende dicho objeto de datos y un conjunto de datos de control, en el que dicho conjunto de datos de control comprende al menos un elemento de control de uso que define un uso del objeto de datos que cumple con las condiciones de control para el uso de un objeto de datos, en el que dicho conjunto de datos de control ha sido adaptado a un usuario específico y comprende al menos un identificador de datos de control que identifica de manera única este conjunto de datos de control de usuario, y en el que el paquete de datos es seguro debido a que el objeto de datos y los elementos de control de uso del conjunto de datos de control de usuario han sido cifrados, en el que el sistema comprende:

medios de comprobación para comprobar si una solicitud por parte de un usuario para usar el objeto de datos cumple o no con el uso definido por el al menos un elemento de control de uso del conjunto de datos de control de usuario,

medios de descifrado y medios de concesión de permiso para descifrar el objeto de datos y permitir el uso solicitado cuando el uso solicitado cumple con el uso definido por el al menos un elemento de control de uso del conjunto de datos de control de usuario, y

medios de denegación de permiso para denegar el permiso del uso solicitado cuando el uso solicitado no cumple con el uso definido por el al menos un elemento de control de uso del conjunto de datos de control de usuario,

en el que los medios de comprobación, de descifrado y concesión de permiso y los medios de denegación de permiso son proporcionados, todos ellos, por un programa de usuario almacenado por un procesador de datos del usuario.

El objeto de datos puede consistir en datos digitales, datos analógicos o una combinación o híbrido de datos analógicos y digitales.

Un conjunto general de datos de control, basado en las condiciones predeterminadas para el uso del objeto de datos, puede ser creado y almacenado en el mismo dispositivo de memoria que el objeto de datos u otro dispositivo de memoria que es accesible por el procesador de datos del proveedor de datos. Las condiciones predeterminadas para el uso pueden ser definidas por el propietario del objeto de datos, por el intermediario o por cualquier otra persona. Pueden diferir entre objetos de datos diferentes.

El conjunto general de datos de control comprende al menos uno o más elementos de control de uso, que definen los usos del objeto de datos que cumplen con las condiciones predeterminadas. Estos usos pueden incluir, por ejemplo, el tipo de usuario, un límite de tiempo para el uso, una zona geográfica para el uso, operaciones permitidas, tales como hacer una copia del objeto de datos o su visionado, y/o reivindicación del pago de royalties. El conjunto general de datos de control puede comprender otros tipos de elementos de control, además del elemento de control de uso. En una realización preferida, el conjunto general de datos de control comprende un elemento de control de seguridad que define un procedimiento de seguridad que tiene que ser realizado antes del uso del objeto de datos.

El conjunto general de datos de control es concatenado con una copia del objeto de datos. De esta manera, los datos de control no residen en el objeto de datos, sino fuera del mismo, lo que hace que los datos de control sean independientes del formato del tipo de objeto de datos y permite un control del uso independientemente del formato del objeto de datos.

Al menos el elemento o los elementos de control del uso y el objeto de datos están cifrados, de manera que el usuario no puede usar el objeto de datos sin un programa de usuario que realice el control de uso y que descifre el objeto de datos. De manera alternativa, todo el conjunto de datos de control y la copia del objeto de datos pueden estar cifrados.

Un usuario puede solicitar autorización para usar un objeto de datos que reside en el procesador de un proveedor de datos a través de una red de datos o de cualquier otra manera apropiada. La autorización puede requerir o no un pago. Cuando se recibe una solicitud de autorización de uso, un conjunto de datos de control de usuario es creado por el procesador del proveedor de datos. El conjunto de datos de control de usuario comprende el conjunto general de datos de control o un subconjunto del mismo, que incluye al menos uno de dichos elementos de control de uso, que es relevante para el usuario actual. También incluye un nuevo identificador que identifica, de manera única, este conjunto de datos de control. Si es relevante, el conjunto de datos de control de usuario comprende también una indicación del número de usos autorizados. Si está autorizado más de un tipo de uso, puede especificarse el número de cada tipo de uso. Por último, el conjunto de datos de control de usuario es concatenado con una copia del objeto de datos, y al menos los elementos de control de uso y la copia del objeto de datos se cifran para crear un paquete de datos seguro preparado para ser transferido al usuario.

Antes de que el paquete de datos sea transferido al usuario, debería confirmarse que se ha accedido a la solicitud de autorización de uso. Preferiblemente, la comprobación se realiza antes de crear el conjunto de datos de control de usuario. Sin embargo, puede realizarse también en paralelo con o después de la creación de los datos de control de usuario. En este último caso, el número de usos solicitados por el usuario se autoriza provisionalmente y se incluye en el conjunto de usuario pero, si la solicitud es denegada, el conjunto de usuario es cancelado o modificado.

El paquete de datos puede ser transferido al usuario mediante medios electrónicos o puede ser almacenado en un medio de almacenamiento masivo y puede ser transferido al usuario por correo o por cualquier medio de transporte adecuado.

Una vez empaquetado el objeto de datos de la manera descrita anteriormente, sólo puede ser accedido por un programa de usuario que tiene un control de uso incorporado y medios para descifrar el paquete de datos. El programa de usuario sólo permitirá los usos definidos como aceptables en los datos de control. Además, si los datos de control comprenden un elemento de control de seguridad, debe cumplirse el procedimiento de seguridad prescrito en el mismo.

En una realización, el control del uso puede realizarse de la manera siguiente. Si el usuario decide usar un objeto de datos, el programa de usuario comprueba los datos de control para ver si esta acción está autorizada. Más particularmente, comprueba que el número de usos autorizados de este tipo sea uno o más. Si es así, la acción se

permite y el número de usos autorizados se decrementa en una unidad. De lo contrario, la acción es interrumpida por el programa de usuario y el usuario puede tener o no la oportunidad de adquirir el derecho de completar la acción.

Después del uso, el programa de usuario vuelve a empaquetar el objeto de datos de la misma manera en la que se empaquetó anteriormente.

Cuando un objeto de datos es redistribuido por un usuario o un intermediario, se añaden nuevos elementos de control en los datos de control para reflejar la relación entre el usuario/intermediario antiguo y el usuario/intermediario nuevo. De esta manera, puede crearse un registro para auditoría para el objeto de datos.

Pueden almacenarse al menos dos paquetes de datos en el procesador de datos de un usuario, el cual examina los elementos de control de uso de los paquetes de datos con el fin de encontrar una coincidencia. Si se encuentra una coincidencia, el procesador de datos del usuario realiza una acción que está especificada en el conjunto de datos de control de usuario. Este procedimiento puede ser usado para vender y comprar objetos de datos.

Breve descripción de los dibujos

La Fig. 1 es un diagrama de flujo que muestra el flujo de datos general según la invención.

La Fig. 2 es un diagrama de bloques de sistema de un procesador de datos de un proveedor de objetos de datos.

La Fig. 3 es un diagrama de bloques que muestra los diferentes módulos de un programa de empaquetado de datos según la invención.

La Fig. 4 es un diagrama de flujo de datos de un procedimiento de empaquetado de datos.

La Fig. 5 es un ejemplo de un archivo de cabecera.

La Fig. 6 es un ejemplo de un archivo de datos de uso.

La Fig. 7 es un diagrama de flujo de datos de la carga de un objeto al procesador de datos del proveedor de objetos de datos.

Las Figs. 8a y 8b son ejemplos de datos de control para un objeto de datos en el procesador de datos del proveedor de objetos de datos y para un objeto preparado para ser transferido a un usuario, respectivamente.

La Fig. 9 es un diagrama de flujo de datos del empaquetado de datos en el procesador de datos del proveedor de objetos de datos.

La Fig. 10 es un diagrama de flujo de un procedimiento de empaquetado de datos.

La Fig. 11 es una imagen de la memoria de un objeto de datos y sus datos de control.

La Fig. 12a es una imagen de la memoria de los datos de control concatenados y el objeto de datos.

La Fig. 12b es una imagen de la memoria de los datos de control concatenados y cifrados y el objeto de datos.

La Fig. 13 es un diagrama de bloques de sistema de un procesador de datos de un usuario.

La Fig. 14 es un diagrama de bloques que muestra los diferentes módulos de un programa de usuario según la invención.

La Fig. 15 es un diagrama de flujo del uso de un objeto de datos en el procesador de datos de un usuario.

La Fig. 16 es un diagrama de flujo de cómo funciona el programa de usuario en un ejemplo de aplicación específico.

La Fig. 17 es un ejemplo de varias estructuras de paquetes de datos para objetos compuestos.

Descripción del mejor modo de llevar a cabo la invención

Panorama General

La Fig. 1 es un diagrama de flujo que muestra el flujo de datos general según la invención. El diagrama de flujo es dividido en una parte 1 de proveedor de objetos de datos y una parte 2 de usuario.

En la parte 1 de proveedor de objetos de datos, un objeto 24 de datos es creado por un autor. El objeto de datos

puede consistir en datos digitales, datos analógicos o una combinación o híbrido de datos analógicos y digitales. La diferencia principal entre los objetos de datos digitales y los objetos de datos analógicos son los medios de almacenamiento, transferencia y uso.

El autor determina también las condiciones 42 para el uso del objeto 24 de datos por parte de un usuario. El objeto 24 de datos y las condiciones 42 de uso son introducidos a un programa 19 de empaquetado de datos, que crea un paquete 40 de datos seguro del objeto de datos y de los datos de control en base a las condiciones 42 de uso introducidas. Una vez empaquetado de esta manera, el objeto de datos sólo puede ser accedido por un programa 35 de usuario.

El objeto de datos puede ser empaquetado junto con un conjunto general de datos de control, que es el mismo para todos los usuarios del objeto de datos. Este puede ser el caso cuando el objeto de datos es enviado a un distribuidor o un boletín, desde donde puede obtenerlo un usuario. El objeto de datos también puede ser empaquetado como consecuencia de una solicitud por parte de un usuario para usar el objeto de datos. En ese caso, el paquete puede incluir datos de control que están adaptados, específicamente, a ese usuario. Estos datos de control se denominan un conjunto de datos de control de usuario. Puede comprender, por ejemplo, el número de usos adquiridos por el usuario. Típicamente, el conjunto de datos de control de usuario se creará en base al conjunto general de datos de control e incluirá al menos un subconjunto de los mismos. Un conjunto de datos de control de usuario no necesita ser adaptado siempre para un usuario específico. Todos los conjuntos de datos de control que se crean en base a un conjunto general de datos de control se denominarán un conjunto de datos de control de usuario. De esta manera, un conjunto de datos de control puede ser un conjunto general en una fase y un conjunto de usuario en otra fase.

El empaquetado de datos indicado anteriormente puede ser realizado por el propio autor mediante el programa 19 de empaquetado de datos. Como alternativa, el autor puede enviar su objeto de datos a un intermediario, el cual introduce el objeto de datos y las condiciones de uso determinadas por el autor al programa 19 de empaquetado de datos con el fin de crear un paquete 3 seguro. El autor puede vender también su objeto de datos al intermediario. En ese caso, el intermediario probablemente desee aplicar sus propias condiciones de uso al programa de empaquetado de datos. El autor puede proporcionar también el objeto de datos en un paquete seguro al intermediario, quien vuelve a empaquetar el objeto de datos y añade datos de control adicionales que son relevantes para sus actividades comerciales. También son concebibles diversas combinaciones de las alternativas anteriores.

En la parte 2 de usuario del diagrama de flujo, el paquete 40 seguro es recibido por un usuario, quien debe usar el programa 35 de usuario con el fin de desempaquetar el paquete 40 seguro y obtener el objeto de datos en una forma 80 final para su uso. Después del uso, el objeto de datos se vuelve a empaquetar en el paquete 40 seguro.

Las diferentes partes del sistema y las diferentes etapas del procedimiento según la invención se describirán ahora más detalladamente.

Procesador de datos del proveedor de datos

La Fig. 2 es un diagrama de bloques de sistema de un procesador de datos de un proveedor de objetos de datos. Tal como se ha indicado anteriormente, el proveedor de objetos de datos puede ser un autor de un objeto de datos, un propietario de un objeto de datos, un intermediario de un objeto de datos o cualquier otra persona que desea distribuir un objeto de datos, al tiempo que conserva el control de su uso. El procesador de datos es un procesador de propósito general o especial, preferiblemente con capacidades de red. Comprende una CPU 10, una memoria 11 y un adaptador 12 de red, que están interconectados por un bus 13. Tal como se muestra en la Fig. 2, otros medios convencionales, tales como una pantalla 14, un teclado 15, una impresora 16, un dispositivo 17 de almacenamiento masivo y una ROM 18, pueden ser conectados también al bus 13. La memoria 11 almacena programas 21 de red y de telecomunicaciones y un sistema 23 operativo (OS). Todos los elementos indicados anteriormente son bien conocidos por las personas con conocimientos en la materia y están disponibles comercialmente. Para el propósito de la presente invención, la memoria 11 almacena también un programa 19 de empaquetado de datos y, preferiblemente, una base 20 de datos destinada para datos de control. Dependiendo del funcionamiento actual, uno o más objetos 24 de datos pueden ser almacenados en la memoria 11, tal como se muestra, o en el almacenamiento 17 masivo. El procesador de datos del proveedor de datos se considera seguro.

Programa de empaquetado de datos

El programa 19 de empaquetado de datos es usado para crear datos de control para controlar el uso de un objeto de datos y para empaquetar el objeto de datos y los datos de control en un paquete seguro.

Tal como se muestra en la Fig. 3, comprende un módulo 301 de control de programa, un módulo 302 de interfaz de usuario, un módulo 303 de empaquetado, un módulo 304 de creación de datos de control, un módulo 305 de

cifrado, uno o más módulos 306 de formato y uno o más módulos 307 de seguridad.

El módulo 301 de control controla la ejecución de los otros módulos. El módulo 302 de interfaz de usuario gestiona la interacción con el proveedor de objetos de datos. El módulo 303 de empaquetado empaqueta los datos de control y el objeto de datos. Usa el módulo 304 de creación de datos de control, los módulos 306 de formato, los módulos 307 de seguridad y el módulo 305 de cifrado tal como se describirá más detalladamente a continuación.

Los módulos 306 de formato comprenden código de programa que es necesario para gestionar los objetos de datos en su formato nativo. Pueden cumplir funciones tales como la compresión de datos y la conversión de datos. Pueden ser implementados mediante cualquier programa apropiado, comercialmente disponible, tal como por medio de una rutina de la biblioteca de compresión de datos para Windows PKWARE Inc. y el paquete Image Alchemy de Handmade Software Incorporated, respectivamente. Pueden ser implementados también mediante programas diseñados a medida.

Los módulos 307 de seguridad comprenden un código de programa necesario para implementar la seguridad, tal como un cifrado más sofisticado que el proporcionado por el módulo 305 de cifrado, algoritmos de autorización, control de acceso y control de uso, por encima y más allá de la seguridad básica inherente en el paquete de datos.

El programa 19 de empaquetado de datos puede contener muchos tipos diferentes de formatos y módulos de seguridad. El módulo 301 de control de programa aplica los módulos de formato y de seguridad solicitados por el proveedor de datos.

El módulo 305 de cifrado puede ser cualquier módulo apropiado, disponible comercialmente, tal como el subprograma de Visual Basic "FileCrypt" que se encuentra en el paquete QuickPak Professional for Windows de Crescent Software - FILECRPT.BAS, o un programa de cifrado de diseño personalizado.

El módulo 304 de creación de datos de control crea los datos de control para controlar el uso del objeto de datos. A continuación, se describirá más detalladamente un ejemplo de una estructura de datos de control.

Datos de control:

Los datos de control pueden ser almacenados en un archivo de cabecera y un archivo de datos de uso. En una realización preferida, el archivo de cabecera comprende campos para almacenar un identificador de objeto, que identifica, de manera única, los datos de control y/o su objeto de datos asociado, un título, un código de formato y un código de seguridad. El código de formato puede representar el formato o la posición de los campos en el archivo de datos de uso. De manera alternativa, el código de formato puede designar uno o más módulos de formato a ser usados por el programa de empaquetado de datos o el programa de usuario. El código de seguridad puede representar el procedimiento de cifrado usado por el módulo 305 de cifrado o cualquier módulo de seguridad a ser usado por el programa de empaquetado de datos y el programa de usuario. Los campos del archivo de cabecera se denominan elementos de encabezado.

El archivo de datos de uso comprende al menos un campo para almacenar datos que controlan el uso del objeto de datos. Uno o más campos de datos de uso que representan una condición para el uso del objeto de datos se denominarán un elemento de uso. En una realización preferida, cada elemento de uso es definido por un campo identificador, por ejemplo, un número de serie, un campo de tamaño, que especifica el tamaño del elemento de uso en bytes o de cualquier otra manera adecuada, y un campo de datos.

Los elementos de cabecera y los elementos de uso son elementos de control que controlan todas las operaciones relacionadas con el uso del objeto. El número de elementos de control es ilimitado. El proveedor de datos puede definir cualquier número de elementos de control para representar sus condiciones de uso predeterminadas del objeto de datos. La única restricción es que el programa 19 de empaquetado de datos y el programa 35 de usuario deben tener código de programa compatible para gestionar todos los elementos de control. Este código de programa reside en el módulo de empaquetado y el módulo de gestión de uso, que se describen a continuación.

Los elementos de control pueden contener datos, secuencia de comandos o código de programa que es ejecutado por el programa 35 de usuario para controlar el uso del objeto de datos relacionado. La secuencia de comandos y el código del programa pueden contener sentencias condicionales y similares, que son procesadas con los objetos y los parámetros de sistema relevantes en el procesador de datos del usuario. También sería posible usar un elemento de control para especificar un programa de usuario propietario específico que sólo puede ser obtenido desde un intermediario particular.

Es evidente que la estructura de datos de control descrita anteriormente es sólo un ejemplo. La estructura de datos de control puede ser definida de muchas formas diferentes con diferentes elementos de control. Por ejemplo, no es obligatoria la partición de los datos de control en datos de cabecera y datos de uso. Además, los elementos de control indicados anteriormente son solo ejemplos. El formato de los datos de control puede ser único, por

ejemplo, diferente para diferentes proveedores de datos, o puede ser definido según un estándar.

Funcionamiento del programa de empaquetado de datos

Ahora, se describirá el funcionamiento de una primera realización del programa de empaquetado de datos con referencia al diagrama de bloques de la Fig. 3 y el diagrama de flujo de la Fig. 4.

En primer lugar, un proveedor de datos crea un objeto de datos y lo salva en un archivo, etapa 401. Cuando el programa de empaquetado de datos es iniciado, etapa 402, el módulo 302 de interfaz de usuario solicita al proveedor de objetos de datos que introduzca, etapa 403, la información de cabecera que consiste, por ejemplo, en un identificador de objeto, un título del objeto de datos, un código de formato que especifica cualquier módulo de formato a usar para convertir el formato del objeto de datos, y un código de seguridad que especifica cualquier módulo de seguridad a ser usado para añadir aún seguridad adicional al objeto de datos. Además, el módulo 302 de interfaz de usuario solicita al proveedor de objetos de datos que introduzca información de uso, por ejemplo, sus condiciones para el uso del objeto de datos. La información de uso puede comprender el tipo de usuario que está autorizado a usar el objeto de datos, el precio de los diferentes usos del objeto, etc. La información de cabecera y la información de uso, que pueden ser introducidas en forma de códigos predeterminados, son pasadas a continuación al módulo 301 de control, que llama al módulo 303 de empaquetado y pasa la información al mismo.

El módulo 303 de empaquetado llama al módulo 304 de creación de datos de control que, en primer lugar, crea un archivo de cabecera, a continuación, crea datos de cabecera en base a la información de cabecera introducida por el proveedor de objetos de datos y, finalmente, almacena los datos de cabecera, etapa 404-405. A continuación, se crea un archivo de datos de uso, en el que los datos de uso son creados en base a la información de uso introducida por el proveedor de datos y, finalmente, los datos de uso son almacenados en el archivo de datos de uso, etapa 406-407.

A continuación, el módulo 303 de empaquetado aplica cualquier formato y los módulos 306, 307 de seguridad especificados en el archivo de cabecera, etapas 408 a 413, al objeto de datos.

A continuación, el módulo 303 de empaquetado concatena el archivo de datos de uso y el objeto de datos y almacena el resultado como un archivo temporal, etapa 414. El módulo 303 de empaquetado llama al módulo 305 de cifrado, que cifra el archivo temporal, etapa 415. El nivel de seguridad dependerá en parte de la calidad de los procedimientos de cifrado y clave usados.

Por último, el módulo 303 de empaquetado concatena el archivo de cabecera y el archivo temporal cifrado y salva el resultado como un único archivo, etapa 416. Este archivo final es el paquete de datos que puede ser distribuido ahora mediante transferencia de archivos a través de una red o en medios de almacenamiento, tales como CD-ROM o disquete, o mediante algún otro medio.

Ejemplo 1

Ahora, se describirá un ejemplo de cómo puede ser usado el programa 19 de empaquetado de datos con referencia a las Figs. 5 y 6. En este ejemplo, el proveedor de objetos de datos es un artista de gráficos por ordenador, que desea distribuir una imagen que puede ser usada como imagen prediseñada, pero sólo en un documento o un archivo que está empaquetado según el procedimiento de la invención y que tiene condiciones de uso que no permiten una edición adicional. El artista quiere proporcionar una vista previa gratuita de la imagen, pero también desea que le paguen en función de cada uso, a menos que el usuario esté dispuesto a pagar un canon bastante sustancial para un uso ilimitado. El artista gestionará el pago y la autorización de uso a través de una línea de acceso telefónico a su procesador de datos.

El artista usa alguna aplicación de creación de imágenes, tal como Photoshop de Adobe para crear su imagen. A continuación, el artista salva la imagen a un archivo en un formato apropiado para su distribución, tal como el formato de intercambio gráfico (Graphical Interchange Format, GIF). A continuación, el artista inicia su programa de empaquetado de datos e introduce un identificador de objeto, un título, un código de formato y un código de seguridad que, en este ejemplo, son "123456789", "imagen", "a" y "b", respectivamente. En este ejemplo, el código de formato "a" indica que no es necesario aplicar ningún código de formato, y se selecciona este código debido a que el formato GIF es apropiado y ya está comprimido. Además, el código de seguridad "b" indica que no se necesita aplicar ningún módulo de seguridad y este código se selecciona debido a que el artista considera que la seguridad conseguida por el cifrado realizado por medio del módulo 305 de cifrado es apropiada.

A continuación, el artista introduce su número de teléfono, su precio para un único uso de la imagen y para un uso ilimitado del objeto de datos, un código para los tipos de uso aprobados y para el número de usos aprobados. Para este propósito, el módulo 302 de interfaz de usuario puede mostrar un formulario de entrada de datos.

El programa 19 de empaquetado de datos crea datos de control en base a la información introducida por el artista y almacena los datos en el archivo de cabecera y en el archivo de datos de uso, tal como se muestra en las Figs. 5 y 6, respectivamente. Estos datos constituyen un conjunto general de datos de control que no está adaptado específicamente a un único usuario, pero que indica las condiciones de uso determinadas por el artista para todos los futuros usuarios.

A continuación, el programa 19 de empaquetado concatena el objeto de datos y los datos de control según las etapas 414-416 de la Fig. 4 para conseguir el paquete seguro. No se aplica ningún módulo de formato o módulo de seguridad al objeto de datos, ya que no son necesarios según los datos en el archivo de cabecera.

Cuando se ha obtenido el paquete seguro, el artista lo envía a un boletín, desde donde puede ser recuperado por un usuario.

Ejemplo 2

A continuación, se describirá otra realización del programa 19 de empaquetado de datos, con referencia a las Figs. 7-12b. En este ejemplo, el objeto de datos consiste en una película de vídeo, que es creada por una empresa cinematográfica y es enviada a un intermediario junto con las condiciones 42 predeterminadas para el uso del vídeo. El intermediario carga el vídeo 24 en el almacenamiento 17 masivo de su procesador de datos. A continuación, usa su programa 19 de empaquetado de datos para crear un conjunto general de datos 50 de control en base a las condiciones 42 predeterminadas para el uso, indicadas por la empresa cinematográfica. Además, la dirección del vídeo en el almacenamiento 17 masivo es almacenada en una tabla de direcciones en la base de datos 20 de control o en otro lugar en la memoria 11. También podría ser almacenada en el conjunto general de datos 50 de control. Finalmente, el conjunto general de datos 50 de control es almacenado en la base de datos 20 de control. También podría ser almacenado en otro lugar en la memoria 11. Después de estas operaciones, que corresponden a las etapas 401-407 de la Fig. 4, se sale del programa de empaquetado de datos.

La Fig. 8a muestra el conjunto general de datos de control para el vídeo según este ejemplo. Aquí, los datos de control incluyen un identificador, un código de formato, un código de seguridad, el número de elementos de uso, el tamaño del objeto de datos, el tamaño de los elementos de uso y dos elementos de uso, comprendiendo cada uno un campo de identificador, un campo de tamaño y un campo de datos. El identificador puede ser un número único en una serie registrada para el intermediario particular. En este ejemplo, el identificador es "123456789", el código de formato "0010", que, en este ejemplo, indica el formato de un vídeo AVI, y el código de seguridad es "0010". Además, el primer elemento de uso define los usuarios aceptables para el vídeo y el segundo elemento de datos de uso define el número de visionados de vídeo adquiridos por un usuario. El primer dato de elemento de uso es 1 que, para los propósitos de este ejemplo, significará que solo los usuarios con orientación educativa son aceptables para la empresa cinematográfica. El campo del dato del segundo elemento de datos de uso está vacío, ya que en esta etapa no se han adquirido visionados de vídeo.

Gestión de transferencia de objetos

El intermediario desea transferir objetos de datos a los usuarios y permitir su uso controlado a cambio del pago de los cánones de uso o royalties. Tanto la gestión de la relación comercial intermediario-usuario como la negociación de la transacción entre el intermediario y el usuario pueden ser automatizadas, y la estructura de datos de control puede proporcionar un soporte ilimitado para estas operaciones. El pago puede ser gestionado mediante la transmisión de información de la tarjeta de crédito, o el usuario puede tener una cuenta de débito o de crédito con el intermediario, activada mediante contraseña. Preferiblemente, el pago debería ser confirmado antes de que el objeto de datos sea transferido al usuario.

Empaquetado de datos:

Cuando un usuario desea usar un objeto de datos, contacta con el intermediario y solicita autorización para el uso del objeto de datos. Cuando el procesador de datos del intermediario recibe la solicitud de autorización, un programa de datos compara el uso para el que se solicita la autorización con los elementos de control de uso de los datos de control del objeto de datos para comprobar si cumple con las condiciones predeterminadas para el uso indicado en los mismos. La comparación puede incluir comparar el tipo de usuario, el tipo de uso, el número de usos, el precio, etc. Si el uso solicitado cumple con las condiciones predeterminadas, se concede la autorización, de lo contrario se deniega.

La Fig. 9 es un diagrama de flujo de datos del empaquetado de datos en el procesador de datos del intermediario, que se produce en respuesta a una solicitud concedida desde un usuario para una autorización para el uso del vídeo, por ejemplo, una solicitud concedida para la adquisición de dos visionados.

En respuesta a una solicitud concedida, el intermediario aplica de nuevo el programa 19 de empaquetado de datos.

El conjunto general de datos 50 de control y el objeto 24 de datos son introducidos al programa desde la base de datos 20 de control y el almacenamiento 17 masivo, respectivamente. El programa crea un conjunto de datos 60 de control de usuario en base al conjunto general de datos 50 de control y concatena el conjunto 60 de usuario y el objeto 24 de datos para crear un paquete 40 de datos seguro que, a continuación, puede ser transferido al usuario mediante cualquier medio adecuado. Preferiblemente, una copia del conjunto de datos de control de usuario es almacenada en la base de datos de control del intermediario. Esto proporciona al intermediario un registro con el cual comparar un uso posterior, por ejemplo, cuando se requiere una conexión telefónica para su uso.

La Fig. 10 es un diagrama de flujo de un procedimiento ejemplar usado para crear un conjunto de datos de control de usuario y para empaquetar el conjunto de datos de control de usuario y el vídeo en un paquete seguro. Aquí, el procedimiento se describirá con referencia al conjunto general de datos de control mostrado en la Fig. 8a.

El conjunto de datos 60 de control de usuario, es decir, un conjunto de datos de control que está adaptado al usuario específico de este ejemplo, es creado en las etapas 1001-1003 de la Fig. 11. En primer lugar, el conjunto general de datos 50 de control almacenados en la base de datos de control es copiado para crear nuevos datos de control, etapa 1001. En segundo lugar, un nuevo identificador, aquí "123456790", que identifica de manera única el conjunto de datos de control de usuario, es almacenado en el campo de identificador de los nuevos datos 60 de control, etapa 1002. En tercer lugar, el campo de datos del segundo elemento de uso es actualizado con el uso adquirido, es decir, en este ejemplo con dos, debido a que se adquirieron dos visionados del vídeo, etapa 1003.

El conjunto de datos de control de usuario, creado de esta manera, que corresponde al conjunto general de datos de control de la Fig. 8a se muestra en la Fig. 8b.

El conjunto de datos de control de usuario es almacenado en la base de datos 20 de control, etapa 1004. A continuación, el vídeo, que está almacenado en el almacenamiento 17 masivo, es copiado, etapa 1005. La copia del video es concatenada con el conjunto de datos de control de usuario, etapa 1006. El código de seguridad 0010 especifica que todo el paquete 40 de datos sea cifrado y que el programa 35 de usuario debe contener una clave que puede ser aplicada. En consecuencia, se cifra todo el paquete de datos, etapa 1007. Finalmente, el paquete de datos cifrado es almacenado en un medio de almacenamiento o es pasado a un programa de red, etapa 1008, para su posterior transferencia al usuario.

La Fig. 11 es una imagen de memoria del video 24 y los datos 60 de control de usuario. Los datos de control de usuario y una copia del vídeo 24 son concatenados, tal como se muestra en la Fig. 12a. El paquete 40 de datos cifrados se muestra en la Fig. 12b.

El procedimiento de la Fig. 10 puede ser implementado mediante el programa de empaquetado de datos de la Fig. 3. Como una alternativa al procedimiento de la Fig. 10, el conjunto de datos de control de usuario puede ser creado como en las etapas 1001-1003 y es salvado en un archivo de cabecera y en un archivo de datos de uso, después de lo cual pueden realizarse las etapas 408-416 del programa de empaquetado de datos de la Fig. 4 para crear el paquete seguro.

El procedimiento descrito anteriormente para crear un conjunto de datos de control adaptado al usuario puede ser usado también por un usuario que desea redistribuir un objeto de datos o por un intermediario que desea distribuir el objeto de datos a otros intermediarios. Obviamente, la redistribución del objeto de datos requiere que la redistribución sea un uso aprobado de los datos de control del objeto de datos. Si es así, el usuario o el intermediario crea un conjunto de datos de control de usuario mediante la adición de nuevos elementos de control y, posiblemente, cambiando los campos de datos del elemento de control antiguo para reflejar la relación entre el autor y el usuario/intermediario actual y entre el usuario/intermediario actual y el usuario/intermediario futuro. De esta manera, se crea un registro para auditoría.

Procesador de datos del usuario

El procesador de datos del usuario, que se muestra en la Fig. 13, es un procesador de propósito general o especial, preferiblemente con capacidades de red. Comprende una CPU 25, una memoria 26 y un adaptador 27 de red, que están interconectados mediante un bus 28. Tal como se muestra en la Fig. 13, otros medios convencionales, tales como una pantalla 29, un teclado 30, una impresora 31, un sistema 32 de sonido, una ROM 33 y un dispositivo 34 de almacenamiento masivo, pueden estar conectados también al bus 28. La memoria 26 almacena programas de red y de telecomunicaciones 37 y un sistema operativo (OS) 39. Todos los elementos indicados anteriormente son bien conocidos por las personas con conocimientos en la materia y están disponibles comercialmente. Para el propósito de la presente invención, la memoria 26 almacena también un programa 35 de usuario y, preferiblemente, una base de datos 36 destinada para los datos de control. Dependiendo de la operación actual, un paquete 40 de datos puede ser almacenado en la memoria 26, tal como se muestra, o en el almacenamiento 34 masivo.

Programa de usuario

El programa 35 de usuario controla el uso de un objeto de datos según los datos de control, que están incluidos en el paquete de datos junto con el objeto de datos.

Tal como se muestra en la Fig. 14, el programa 35 de usuario comprende un módulo 1401 de control de programa, un módulo 1402 de interfaz de usuario, un módulo 1403 gestor de uso, un módulo 1404 de analizador de datos de control, un módulo 1405 de descifrado, uno o más módulos 1406 de formato, uno o más módulos 1407 de seguridad y un programa 1409 de transferencia de archivos.

El módulo 1401 de control controla la ejecución de los otros módulos. El módulo 1402 de interfaz de usuario gestiona las interacciones con el usuario. El módulo 1403 gestor de uso desempaqueta el paquete 40 seguro. Usa el módulo 1404 analizador de datos de control, el módulo 1405 de descifrado, los módulos 1406 de formato y los módulos 1407 de seguridad.

Los módulos 1406 de formato comprenden código de programa, que es necesario para gestionar los objetos de datos en su formato nativo, tal como los procedimientos de descompresión y de formato de datos. Los módulos 1407 de seguridad comprenden código de programa necesario para implementar la seguridad por encima del nivel más bajo, tal como control de acceso, control de uso y un descifrado más sofisticado que el proporcionado por el módulo 1405 de descifrado básico.

El programa 35 de usuario puede contener muchos tipos diferentes módulos de formato y de seguridad. Sin embargo, deberían ser complementarios con los módulos de formato y de seguridad usados en el programa de empaquetado de datos correspondiente. El módulo 1401 gestor de uso aplica los módulos de formato y de seguridad que son necesarios para usar un objeto de datos y que se especifican en sus datos de control. Si los módulos de formato y de seguridad apropiados no están disponibles para un objeto de datos particular, el módulo 1401 gestor de uso no permitirá ningún uso.

El módulo 1405 de descifrado puede ser el subprograma de Visual Basic FileCrypt, indicado anteriormente, o algún otro programa de descifrado disponible comercialmente. Puede ser también un módulo de descifrado diseñado a medida. La única restricción es que el módulo de descifrado usado en el programa de usuario sea complementario con el módulo de cifrado del programa de empaquetado de datos.

El módulo 1403 analizador de datos de control realiza el procedimiento inverso del módulo 304 de creación de datos de control en la Fig. 3.

El programa 35 de usuario puede tener código que controla el uso del programa mediante contraseña o mediante cualquier otro procedimiento adecuado. Puede añadirse una contraseña en un elemento de control de contraseña durante el empaquetado del objeto de datos. La contraseña es transferida al usuario por correo certificado o por cualquier otro medio apropiado. En respuesta a la presencia del elemento de control de contraseña en la estructura de datos de control, el programa de usuario solicita al usuario que introduzca la contraseña. La contraseña introducida es comparada con la contraseña en los datos de control y, si coinciden, el programa de usuario continúa, de lo contrario, es desactivado.

El programa 35 de usuario puede tener también procedimientos que alteran el comportamiento del programa (por ejemplo, proporcionan filtros para niños) según los datos de control del objeto 41 de usuario. Es importante mencionar que el programa 35 de usuario nunca almacena el objeto en formato nativo en el almacenamiento accesible al usuario y que, durante el visionado del objeto de datos, la tecla de imprimir pantalla está desactivada.

El programa 1409 de transferencia de archivos puede transferir y recibir archivos a través de la red hacia y desde otro procesador de datos.

Debido a que el objeto de datos se vuelve a empaquetar en el paquete seguro tras el uso, el programa de usuario debería incluir también código de programa para volver a empaquetar el objeto de datos. El código de programa podría ser el mismo que el usado en el programa 19 de empaquetado de datos correspondiente. También podría ser un programa independiente al que se llama desde el programa de usuario.

Funcionamiento del programa de usuario:

Ahora, se describirá el funcionamiento de una realización del programa 35 de usuario, con referencia al diagrama de bloques de la Fig. 14 y el diagrama de flujo de la Fig. 15.

En primer lugar, el usuario recibe un paquete 40 de datos a través de una transferencia de archivos a través de una red o en un medio de almacenamiento, tal como CD-ROM o disquete, o mediante cualquier otro medio apropiado, etapa 1501. A continuación, almacena el paquete de datos como un archivo en su procesador de datos,

etapa 1502.

Cuando el usuario desea usar el objeto de datos, inicia el programa 35 de usuario, etapa 1503. A continuación, solicita el uso del objeto de datos, etapa 1504. La solicitud es recibida por el módulo 1402 de interfaz de usuario, que notifica al módulo 1401 de control la solicitud de uso. El módulo 1401 de control llama al módulo 1403 gestor de uso y pasa la solicitud de uso.

El módulo 1403 gestor de uso lee el código de formato desde el paquete de datos para determinar el formato de los datos de control. A continuación, llama al módulo 1405 de descifrado para descifrar y extraer los datos de control desde el paquete de datos. El módulo 1403 gestor de uso aplica el módulo 1405 de descifrado de manera incremental para descifrar solo los datos de control. Finalmente, almacena los datos de control en memoria, etapa 1505.

A continuación, el módulo 1403 gestor de uso llama al módulo 1404 analizador de datos de control para extraer los campos de datos desde los elementos de uso.

A continuación, el módulo 1403 gestor de uso compara la solicitud del usuario para el uso con los datos de control correspondientes, etapas 1506-1507. Si no se permite el uso solicitado en los datos de control, el uso solicitado se deshabilita, etapa 1508. Sin embargo, si el uso solicitado está aprobado en los datos de control, el módulo 1403 gestor de uso aplica cualquier módulo 1406, 1407 de formato y seguridad especificados en los datos de cabecera o los datos de uso, etapas 1509-1514, al paquete de datos.

A continuación, el módulo 1403 gestor de uso llama al módulo 1405 de descifrado, que descifra los datos del objeto, etapa 1515, tras lo cual el uso solicitado es habilitado, etapa 1516. En conexión con la habilitación del uso, es posible que los datos de control necesiten ser actualizados, etapa 1517. Los datos de control pueden comprender, por ejemplo, un campo de datos que indica un número limitado de usos. Si es así, este campo de datos es decrementado en una unidad en respuesta a la habilitación del uso. Cuando el usuario ha terminado el uso del objeto de datos, el programa 35 de usuario restaura el paquete de datos en la forma segura volviéndolo a empaquetar, etapa 1518. Más particularmente, el objeto de datos y los elementos de uso se vuelven a concatenar y cifrar. A continuación, se añaden los elementos de cabecera y el paquete creado de esta manera es almacenado en el procesador de datos del usuario.

Ejemplo 1 Continuación

Ahora, se describirá un ejemplo específico de cómo funciona el programa de usuario, con referencia a las Figs. 6 y 15. El ejemplo es una continuación del ejemplo 1 anterior, en el que un artista ha creado una imagen y la ha enviado a un boletín.

Supóngase que un usuario ha encontrado la imagen en un boletín electrónico (BBS) y está interesado en usarla. Entonces, carga el paquete 40 de datos que contiene la imagen a su procesador de datos y lo almacena como un archivo en el almacenamiento masivo. A continuación, el usuario ejecuta el programa 35 de usuario y solicita una visualización previa de la imagen. A continuación, el programa de usuario realiza las etapas 1505-1507 del diagrama de flujo en la Fig. 15. La solicitud de una vista previa de la imagen es comparada con el campo de datos del elemento de uso "código para el tipo de uso aprobado". En este ejemplo, el código "9" indica que se permiten vistas previas. De esta manera, la vista previa solicitada es OK. A continuación, el programa 35 de usuario realiza la etapa 1509-1515 de la Fig. 15. Debido a que el código de formato "a" y el código de seguridad "b" de los datos de cabecera indican que no se requiere ni tratamiento de conversión, ni de descompresión, ni de seguridad, el programa de usuario sólo descifra los datos del objeto. A continuación, el módulo 1403 gestor de uso muestra la vista previa en el procesador de datos del usuario y devuelve el control a la interfaz 1402 de usuario.

Cuando el usuario ha terminado la vista previa de la imagen, el módulo 1402 de interfaz de usuario muestra los costes del uso de la imagen según los datos de los precios de uso de los datos de control ("precio para un solo uso" y "precio para uso ilimitado" en la Fig. 6) y solicita al usuario que introduzca una solicitud de adquisición. El usuario decide comprar un uso ilimitado de la imagen, y el módulo 1402 de interfaz de usuario introduce información de adquisición, tal como identificación, facturación y dirección para esa solicitud y pasa la solicitud al módulo 1401 de control. El módulo de control llama al programa 1409 de transferencia de archivos, que marca el número telefónico del artista, tal como se indica en los datos de uso ("elemento de control para el número de teléfono del artista" en la Fig. 6) y transfiere la solicitud y la información de adquisición a un programa de intermediación en el procesador de datos del artista. Tras la aprobación de la adquisición, el programa de intermediación devuelve un archivo que contiene una actualización para elementos de control "tipo de uso aprobado". La actualización es "10" para el tipo de uso aprobado que, en este ejemplo, indica que se permite el uso ilimitado por parte de ese usuario. El programa 1409 de transferencia de archivos pasa esta actualización al módulo 1403 gestor de uso que actualiza los datos de control con el código "tipo de uso aprobado". A continuación, el módulo 1402 de interfaz de usuario muestra un mensaje de confirmación al usuario.

Posteriormente, el módulo de interfaz de usuario introduce una solicitud para copiar la imagen a un archivo empaquetado según la presente invención, en la máquina del usuario. A continuación, el módulo gestor de uso compara los datos de control de la solicitud del usuario. El módulo gestor de uso examina el campo de datos para el "tipo de uso aprobado", que ahora es "10". El módulo gestor de uso copia la imagen al archivo.

Cuando el usuario ha terminado con la imagen, el módulo 1403 gestor de uso vuelve a empaquetar la imagen como anteriormente excepto con los datos de control actualizados. Este procedimiento de re-empaquetado es exactamente igual que el mostrado en la Fig. 4, excepto que la cabecera y los datos de uso ya existen, de manera que el procedimiento empieza después de la etapa 406, en la que se crean los datos de control.

Seguridad mejorada

Si el proveedor de objetos de datos desea mejorar la seguridad de un paquete de datos que contiene un objeto de datos, podría usarse un módulo 307 de seguridad que contiene un sofisticado algoritmo de cifrado, tal como RSA. En ese caso, el módulo 303 de empaquetado llama al módulo 307 de seguridad en la etapa 412 del diagrama de flujo de la Fig. 4. El módulo de seguridad cifra la imagen y pasa un código de algoritmo de seguridad al módulo 302 de creación de datos de control, que añade un elemento de control para el código del módulo de seguridad, el cual será detectado por el programa 35 de usuario. A continuación, el empaquetado de datos continúa con la etapa 414. Cuando el paquete de datos es enviado al usuario, la clave pública es enviada al usuario por correo certificado. Cuando el programa de usuario es ejecutado en respuesta a una solicitud de uso de este objeto de datos, el módulo gestor de uso detectará el código del módulo de seguridad en los datos de control y llamará al módulo de seguridad. Este módulo transfiere el control al módulo 1402 de interfaz de usuario, que solicita al usuario que introduzca la clave pública. Si la clave es correcta, el módulo de seguridad de usuario aplica un descifrado complementario usando esa clave y pasa un mensaje de uso aprobado al módulo gestor de uso, que permite el uso.

Como otro ejemplo de seguridad mejorada, un módulo de seguridad puede implementar un procedimiento de autorización, según el cual cada uso del objeto de datos requiere una marcación al procesador de datos del proveedor de objetos de datos. Cuando el código de módulo de seguridad correspondiente es detectado por el programa 35 de usuario, se llama al módulo de seguridad relevante. Este módulo pasa una solicitud de autorización al módulo 1401 de control, que llama al programa 1409 de transferencia de archivos, el cual marca el número de acceso telefónico del proveedor de objetos de datos, que está indicado en un elemento de uso y transfiere la solicitud de autorización de uso. Después de una autorización concedida, el procesador de datos del proveedor de datos devuelve un mensaje de uso aprobado al módulo de seguridad de usuario, que envía la aprobación al módulo de control del uso, que permite un uso. Si el usuario solicita usos adicionales del objeto de datos, el procedimiento de autorización es repetido. Este procedimiento resulta en una seguridad permanente del objeto de datos.

Ejemplo 2 Continuación

Ahora, se describirá un ejemplo adicional específico de cómo funciona el programa 35 de usuario, con referencia a la Fig. 16. El ejemplo es una continuación del ejemplo 2 anterior, en el que un usuario adquirió dos visionados de una película de vídeo desde un intermediario.

El usuario desea reproducir el vídeo que fue adquirido y transferido desde el intermediario. El usuario aplica el programa 35 de usuario, etapa 1601, y solicita la reproducción del video, etapa 1602. El programa 35 de usuario examina, en primer lugar, el conjunto de datos 60 de control de usuario, etapa 1603. En este ejemplo, el programa 35 de usuario contiene sólo aquellos módulos de formato y de seguridad para los objetos con código de formato de 0010 y con un código de seguridad de 0010. En consecuencia, sólo pueden usarse esos tipos de objetos de datos. Si el programa encuentra otros códigos, no permitirá la acción de uso, etapa 1604-05.

A continuación, el programa 35 de usuario compara el primer dato de elemento de control, que es 1, sólo para usuarios educativos, con la información de usuario introducida por el usuario a solicitud del programa de usuario. Debido a que el tipo de usuario introducido por el usuario es el mismo que el indicado en el primer elemento de uso, el procedimiento continúa, etapas 1606-1607. A continuación, el programa de usuario comprueba el segundo dato de elemento de control que especifica que el número de reproducciones adquiridas es 2. En consecuencia, el uso es habilitado, etapa 1609. El programa de usuario aplica el módulo de descifrado con la clave universal y el formato de vídeo AVI es visualizado en la unidad 29 de visualización. A continuación, el segundo dato de elemento de control se decrementa en una unidad, etapa 1610. Por último, el vídeo se vuelve a empaquetar, etapa 1611.

Implementación de control de objeto variable y extensible:

El control de objeto se consigue mediante la interacción del programa 19 de empaquetado de datos y el programa 35 de uso con los datos de control. La variación del control del objeto puede aplicarse a un objeto particular

mediante la creación de un formato de datos de control con elementos de control que definen la variación de control y las circunstancias en las que se aplica la variación. A continuación, los procedimientos de programa deberían ser añadidos a los módulos del programa para procesar los elementos de control. Por ejemplo, supóngase que un intermediario desea permitir que los estudiantes impriman un determinado artículo de manera gratuita, pero desea que los usuarios con orientación empresarial paguen por ello. Define elementos de control para representar los tipos estudiante y empresarial y los costes asociados para cada uno. A continuación, añade lógica de programa para examinar el tipo de usuario y calcular los costos en consecuencia. El control de objetos es extensible en el sentido de que el formato de los datos de control puede tener tantos elementos como parámetros hay que definen las normas para el control de objetos.

Implementación de seguridad de objetos variable y extensible

La seguridad del objeto se consigue también mediante la interacción del programa 19 de empaquetado de datos y el programa 35 de usuario con los datos de control. El procedimiento de seguridad y los algoritmos de cifrado/descifrado pueden ser añadidos como módulos de programa. La variación de la seguridad del objeto puede ser aplicada a un objeto particular mediante la creación de un formato de datos de control con elementos de control que definen la variación de seguridad y las circunstancias en las que se aplica la variación. Deberían añadirse procedimientos de programa a los módulos de programa para procesar los elementos de control. Por ejemplo, supóngase que un intermediario desea aplicar una seguridad mínima a su colección de artículos de prensa actuales, pero desea aplicar fuertes medidas de seguridad a su enciclopedia y libros de texto. Define un elemento de control para el tipo de seguridad. A continuación, añade lógica de programa para aplicar los algoritmos de seguridad en consecuencia. La seguridad del objeto es extensible en el sentido de que pueden aplicarse múltiples niveles de seguridad. Por supuesto, el nivel de seguridad dependerá del procedimiento de cifrado/claves implementado en los módulos de seguridad. Un nivel de seguridad puede requerir confirmación en línea al cargar un objeto de datos al procesador de datos del usuario. Esto puede implementarse en el código de programa en un módulo de seguridad. Esto permite que el intermediario compruebe que el objeto no ha sido cargado ya, y realice una doble comprobación del resto de parámetros.

También es importante tener un control de versiones con sello de tiempo entre el programa de uso y la base de datos de control del usuario. De lo contrario, la base de datos puede ser duplicada y aplicada de nuevo al programa de usuario. El programa de usuario puede colocar un sello de tiempo en la base de datos de control y en un archivo oculto del sistema cada vez que se accede a la base de datos de control. Si los sellos de tiempo no son idénticos, la base de datos de control ha sido manipulada y se deshabilita todo uso. El código de programa para gestionar los sellos de tiempo puede residir en un módulo de seguridad.

Gestión de objetos compuestos:

Un objeto compuesto puede ser gestionado definiendo un formato de datos de control con elementos de control que definen relaciones entre los objetos constitutivos y definiendo un elemento padre/hijo y un elemento de id del objeto relacionado. Por ejemplo, supóngase que un intermediario desea incluir un video y un libro de texto en un paquete educativo. Crea un objeto padre con elementos de control que hacen referencia a objetos de vídeo y libros de texto. También incluye elementos de control en los datos de control para el objeto de vídeo y el objeto libro de texto con referencia al objeto padre. Por último, añade procedimientos de programa a módulos de programa para procesar los elementos de control.

En otras palabras, cuando el objeto de datos es un objeto de datos compuesto que incluye al menos dos objetos de datos constitutivos, se crea un conjunto general de datos de control respectivo para cada uno de entre el objeto de datos constitutivo y el objeto de datos compuesto. En respuesta a una solicitud desde un usuario, se crea un conjunto de datos de control de usuario respectivo para cada uno de los objetos de datos constitutivos, así como para el objeto de datos compuesto.

En la Fig. 17 se proporcionan ejemplos de diversas estructuras de paquetes de datos para objetos compuestos.

Otro aspecto de los objetos compuestos es cuando el usuario desea combinar objetos de datos para algún uso particular. La combinación es una acción de uso que debe ser permitida en cada objeto de datos constitutivo. Se crea un nuevo objeto de datos con datos de control que unen los objetos de datos constitutivos. Cada objeto de datos constitutivo conserva sus datos de control originales, que continúan controlando su uso subsiguiente.

Cuando un usuario solicita autorización para el uso de un objeto de datos constitutivo en un objeto de datos compuesto, se crea un conjunto de datos de control de usuario sólo para ese objeto de datos constituyente y es concatenado sólo con una copia de ese objeto de datos constitutivo.

Implementación escalable

La estructura flexible de los datos de control y la estructura modular del programa permiten una extensibilidad casi ilimitada con respecto a la implementación de los requisitos del propietario para el control del uso y el pago de royalties. La estructura de datos de control puede incluir elementos de control para tipos complejos de usuario, tipos de uso, múltiples esquemas de facturación, requisitos de crédito artístico o de propiedad y otros. Pueden incluirse módulos de seguridad que interactúan con cualquier variación de la estructura de los datos de control y los datos de control. Los módulos de seguridad podrían requerir el establecimiento de una marcación al procesador de datos del intermediario para aprobar la carga o las acciones de uso e implementar mecanismos de autenticación de aprobación.

Usuario actuando como un intermediario

Una implementación limitada o completa del programa de empaquetado de datos del intermediario puede ser implementada en la máquina del usuario para permitir una distribución o reventa adicional. Sin embargo, sólo aquellos objetos de datos con datos de control que permiten una distribución o reventa adicional están habilitados de esa manera.

Re-intermediación

Un autor de un objeto de datos puede desear permitir que su intermediario original distribuya su objeto de datos a otros intermediarios, los cuales también distribuirán su imagen. Entonces, incluye un elemento de control que permite la re-intermediación en los datos de control antes de distribuir el objeto de datos con sus datos de control asociados al intermediario original. Cuando se solicite para una re-intermediación, el intermediario original copia el conjunto general de datos de control y actualiza la copia para crear un conjunto de datos de control de usuario que funcionará como el conjunto general de datos de control en el procesador de datos del intermediario subsiguiente. El intermediario original empaqueta el objeto de datos con el conjunto de datos de control de usuario y transfiere el paquete al intermediario subsiguiente. A continuación, el intermediario subsiguiente procede como si fuera un intermediario original.

Negociación automatizada de transacciones

Este es un ejemplo de cómo las condiciones predeterminadas para el uso, incluidas en los datos de control, pueden ser usadas para conseguir una negociación automatizada de transacciones.

Supóngase que una empresa desea ofrecer un equipo automatizado de compra/venta de acciones. Las órdenes de compra y venta podrían ser implementadas en forma de paquetes de datos y un programa de usuario podría procesar los paquetes de datos y ejecutar las transacciones. Los paquetes de datos podrían transportar dinero digital y gestionar el pago en base a las condiciones definidas en los datos de control.

En este ejemplo, la orden de compra es creada usando un programa de empaquetado de datos según la invención en el procesador de datos del comprador. La orden de venta es creada usando el programa de empaquetado de datos en el procesador de datos del vendedor. Ambas órdenes son usadas por el programa de usuario en el procesador de datos del operador de acciones. Los usos tendrían la forma de usar un paquete de datos de orden de venta para vender acciones y un paquete de datos de orden de compra para comprar acciones. Las reglas o condiciones de compra y venta de acciones podrían estar indicadas en los datos de control de los paquetes. El objeto de datos consiste en dinero digital. En este contexto, es importante recordar que el dinero digital es simplemente un grupo de datos que hace referencia a dinero real o dinero virtual emitido y mantenido con el propósito de realizar transacciones digitales.

En este ejemplo, el comprador comienza con un archivo de datos de dinero digital. Usa el programa de empaquetado de datos para crear los datos de control, por ejemplo, tipo de acciones, precio, cantidad, para la compra y, a continuación, empaqueta el archivo de datos de dinero digital y los datos de control en un paquete seguro, tal como se ha descrito anteriormente.

El vendedor comienza con un archivo de datos vacío. Este archivo vacío es similar al archivo de datos de dinero digital, salvo que está vacío. El vendedor crea los datos de control, por ejemplo, tipo de acciones, precio, cantidad y empaqueta el archivo vacío y los datos de control en un paquete seguro.

Tanto el paquete de orden de venta como el paquete de orden de compra son transferidos al procesador de datos de la empresa operadora de acciones, en el que son recibidas y almacenadas en la memoria. El programa de usuario de la empresa operadora de acciones examina los datos de control de los paquetes de orden de compra y de orden de venta de la misma manera que se ha descrito anteriormente y busca una coincidencia. Tras identificar órdenes de compra y venta coincidentes, el programa de usuario ejecuta una transacción, de manera que el dinero digital es extraído del paquete de datos de orden de compra y es trasladado al paquete de orden de venta. A continuación, los datos de control de los paquetes de datos son actualizados para proporcionar un registro para

auditoría. Ambos paquetes se vuelven a empaquetar de la misma manera en la que fueron empaquetados anteriormente y, a continuación, son trasferidos de nuevo a sus autores.

La técnica descrita anteriormente podría ser usada para vender y comprar cualquier objeto, así como para negociaciones automatizadas. El pago puede realizarse de otras maneras diferentes al dinero digital.

En el caso general, el procesador de datos del usuario descifra los elementos de control de uso a partir de los conjuntos de datos de control de usuario y examina los elementos de control de uso para encontrar una coincidencia. En respuesta al hallazgo de una coincidencia, el procesador de datos del usuario realiza una acción especificada en el conjunto de datos de control de usuario.

REIVINDICACIONES

1. Un procedimiento para controlar el uso de un objeto de datos con el fin de cumplir con las condiciones de control para el uso del objeto (24) de datos, en el que el objeto de datos está contenido dentro de un paquete de datos que comprende dicho objeto de datos y un conjunto de datos de control, en el que dicho conjunto de datos de control comprende al menos un elemento de control de uso que define un uso del objeto de datos que cumple con las condiciones de control para el uso de un objeto de datos, en el que dicho conjunto de datos de control ha sido adaptado a un usuario específico y comprende al menos un identificador de datos de control que identifica, de manera única, este conjunto de datos (60) de control de usuario, y en el que el paquete (40) de datos es seguro, ya que el objeto de datos y los elementos de control de uso del conjunto de datos de control de usuario han sido cifrados, en el que el procedimiento comprende:

comprobar (1506), en respuesta a una solicitud por parte de un usuario para usar el objeto de datos, si el uso solicitado cumple o no con el uso definido por el al menos un elemento de control de uso del conjunto de datos de control de usuario, y

en respuesta a si el uso solicitado cumple o no con el uso definido por el al menos un elemento de control de uso del conjunto de datos de control de usuario, descifrar (1515) el objeto de datos y permitir (1516) el uso solicitado,

en el que las etapas de comprobación, descifrado y concesión de permiso son realizadas por un programa (35) de usuario almacenado por un procesador de datos del usuario,

y en el que el programa (35) de usuario no permitirá ningún uso del objeto de datos cuando el uso solicitado no cumpla con dicho uso definido.

2. Procedimiento para controlar el uso de un objeto de datos según la reivindicación 1, en el que los usos del objeto (24) de datos definidos por el uno o más elementos de control de uso comprenden uno o más de entre: el tipo de usuario, un límite de tiempo para el uso, una zona geográfica para el uso, operaciones permitidas, el número de usos autorizado, el precio y la redistribución.

3. Procedimiento para controlar el uso de un objeto de datos según la reivindicación 2, en el que las operaciones permitidas incluyen uno o más de entre: visionar el objeto de datos, usar el objeto de datos, imprimir el objeto de datos y copiar el objeto (24) de datos.

4. Procedimiento para controlar el uso de un objeto de datos según la reivindicación 2 o la reivindicación 3, en el que los usos del objeto (24) de datos comprenden una indicación del número de veces que el usuario está autorizado a usar el objeto de datos según al menos un elemento de control de usuario; en el que el procedimiento comprende, además, sólo permitir el uso solicitado del objeto de datos cuando dicho número de veces es uno o más, y decrementar el número de veces en una unidad cuando se permite el uso solicitado.

5. Procedimiento para controlar el uso de un objeto de datos según cualquiera de las reivindicaciones anteriores, en el que el elemento de control de uso es actualizado después del uso del objeto (24) de datos.

6. Procedimiento para controlar el uso de un objeto de datos según cualquiera de las reivindicaciones anteriores, en el que el programa (35) de usuario nunca almacena el objeto (24) de datos en formato nativo en un almacenamiento accesible por el usuario, y el procedimiento comprende además volver a empaquetar el objeto de datos en el paquete (40) de datos seguro después del uso.

7. Procedimiento para controlar el uso de un objeto de datos según cualquiera de las reivindicaciones anteriores, en el que el conjunto de datos de control de usuario comprende un elemento de control de seguridad, y comprende además la etapa (1514) de llevar a cabo, antes de cada uso del objeto de datos, un procedimiento (1007, 1514) de seguridad definido en el elemento de control de seguridad.

8. Procedimiento para controlar el uso de un objeto de datos según la reivindicación 7, en el que la etapa de comprobar si el uso solicitado cumple con el uso definido por el al menos un elemento de control de uso comprende la etapa de comprobar que el procesador de datos del usuario (Fig. 13) es capaz de llevar a cabo el procedimiento (1007, 1514) de seguridad especificado en el elemento de control de seguridad del conjunto de datos de control de usuario y, si no, no se permite el uso.

9. Procedimiento para controlar el uso de un objeto de datos según cualquiera de las reivindicaciones anteriores, que comprende las etapas adicionales de volver a concatenar, después del uso del objeto (24) de datos, el objeto de datos y el uno o más elementos de control de uso, volver a cifrar al menos el objeto de datos y el uno o más elementos de control de uso, y almacenar el paquete (1518, 1611) de datos re-empaquetado de esta manera en la memoria (26) del procesador de datos del usuario.

10. Procedimiento para controlar el uso de un objeto de datos según cualquiera de las reivindicaciones anteriores, en el que el conjunto de datos (60) de control de usuario comprende un subconjunto de un conjunto general de datos (50) de control.

11. Procedimiento para controlar el uso de un objeto de datos según cualquiera de las reivindicaciones 1 a 9, en el que el conjunto de datos (60) de control de usuario comprende un conjunto general de datos (50) de control.

12. Procedimiento para controlar el uso de un objeto de datos según la reivindicación 10 o la reivindicación 11, en el que dicho conjunto (60) de datos de control de usuario ha sido creado mediante las etapas:

copiar un conjunto general de datos (50) de control para crear nuevos datos de control (1001),

almacenar el identificador de datos de control, que identifica de manera única el conjunto de datos de control de usuario en el conjunto general de datos de control copiado (1002), y

actualizar el conjunto general de datos de control copiado para incluir elementos de control de uso que definen los usos adquiridos por el usuario particular (1003).

13. Procedimiento para controlar el uso de un objeto de datos según la reivindicación 12, en el que el usuario particular ha adquirido usos mediante las etapas de: recibir en un procesador (10) de datos de un proveedor de objetos de datos una solicitud de autorización para el uso por un usuario; comparar el uso para el que se solicita la autorización con uno o más elementos de control de uso del conjunto general de datos (50) de control, y conceder la autorización si el uso para el cual se solicita la autorización cumple con los usos definidos por dicho uno o más elementos de control de uso.

14. Procedimiento para controlar el uso de un objeto de datos según la reivindicación 13, en el que se ha realizado un etapa de garantizar un pago por la autorización solicitada para el uso antes de conceder la autorización.

15. Un sistema para controlar el uso de un objeto de datos con el fin de cumplir con las condiciones de control para el uso del objeto (24) de datos, en el que el objeto de datos está contenido dentro de un paquete de datos que comprende dicho objeto de datos y un conjunto de datos de control, en el que dicho conjunto de datos de control comprende al menos un elemento de control de uso que define un uso del objeto de datos que cumple con las condiciones de control para el uso de un objeto de datos, en el que dicho conjunto de datos de control ha sido adaptado a un usuario específico y comprende al menos un identificador de datos de control que identifica de manera única este conjunto de datos (60) de control de usuario, y en el que el paquete (40) de datos es seguro, ya que el objeto de datos y los elementos de control de uso del conjunto de datos de control de usuario han sido cifrados, en el que el sistema comprende:

medios (1403) de comprobación para comprobar si una solicitud por parte de un usuario para usar el objeto de datos cumple o no con el uso definido por el al menos un elemento de control de uso del conjunto de datos de control de usuario,

medios (1403, 1405) de descifrado y de concesión de permiso para descifrar el objeto de datos y permitir el uso solicitado cuando el uso solicitado cumple con el uso definido por el al menos un elemento de control de uso del conjunto de datos de control de usuario, y

medios (1401, 1403) de denegación de permiso para denegar el permiso del uso solicitado cuando el uso solicitado no cumple con el uso definido por el al menos un elemento de control de uso del conjunto de datos de control de usuario,

en el que los medios de comprobación, descifrado y concesión de permiso y los medios de denegación de permiso son proporcionados, todos ellos, por un programa (35) de usuario almacenado por un procesador de datos del usuario.

16. Sistema para controlar el uso de un objeto de datos según la reivindicación 15, en el que los usos del objeto (24) de datos definidos por el uno o más elementos de control de uso comprenden uno o más de entre: el tipo de usuario, un límite de tiempo para el uso, una zona geográfica para el uso, operaciones permitidas, el número de usos autorizado, el precio y la redistribución.

17. Sistema para controlar el uso de un objeto de datos según la reivindicación 16, en el que las operaciones permitidas incluyen uno o más de entre: visionar el objeto de datos, usar el objeto de datos, imprimir el objeto de datos y copiar el objeto (24) de datos.

18. Sistema para controlar el uso de un objeto de datos según la reivindicación 16 o la reivindicación 17, en el que los usos del objeto (24) de datos comprenden una indicación del número de veces que el usuario está autorizado a

usar el objeto de datos según al menos un elemento de control de usuario, en el que dicho programa (35) de usuario sólo permite el uso solicitado del objeto de datos cuando dicho número de veces es uno o más, y un módulo (1403) gestor de uso de dicho programa (35) de usuario decrementa el número de veces en una unidad cuando se permite el uso solicitado.

19. Sistema para controlar el uso de un objeto de datos según cualquiera de las reivindicaciones 15 a 18, en el que dicho programa (35) de usuario está dispuesto para actualizar el elemento de control de uso después del uso del objeto (24) de datos.

20. Sistema para controlar el uso de un objeto de datos según cualquiera de las reivindicaciones 15 a 19, en el que el programa (35) de usuario nunca almacena el objeto (24) de datos en formato nativo en un almacenamiento accesible por el usuario, y el programa (35) de usuario está dispuesto para volver a empaquetar el objeto de datos en el paquete (40) de datos seguro después del uso.

21. Sistema para controlar el uso de un objeto de datos según cualquiera de las reivindicaciones 15 a 20, en el que el conjunto de datos de control de usuario comprende un elemento de control de seguridad, y el sistema comprende además módulos (1407) de seguridad dispuestos para realizar, antes de cada uso del objeto de datos, un procedimiento (1007, 1514) de seguridad definido en el elemento de control de seguridad.

22. Sistema para controlar el uso de un objeto de datos según cualquiera de las reivindicaciones 15 a 21, en el que el programa (35) de usuario comprende un módulo (1401) de control del programa, un módulo (1402) de interfaz de usuario, un módulo (1403) gestor de uso, un módulo (1404) analizador de datos de control, un módulo (1405) de descifrado, uno o más módulos (1406) de formato, uno o más módulos (1407) de seguridad y un programa (1409) de transferencia de archivos.

Fig 1

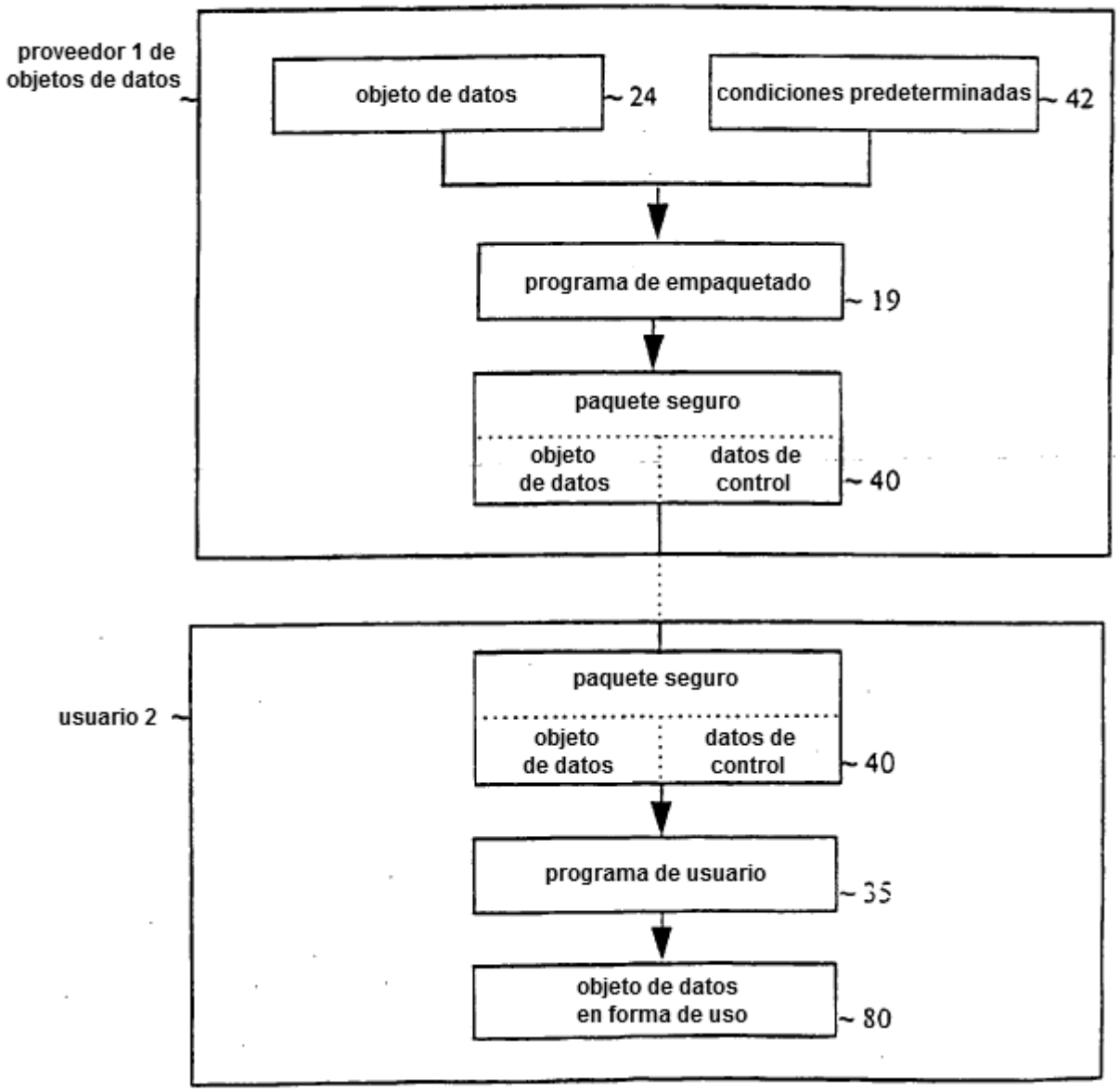

proveedor 1 de objetos de datos
objeto de datos
24
condiciones predeterminadas
42
programa de empaquetado
19
paquete seguro
objeto de datos
datos de control
40
usuario 2
paquete seguro
objeto de datos
datos de control
40
programa de usuario
35
objeto de datos en forma de uso
80

Fig 2

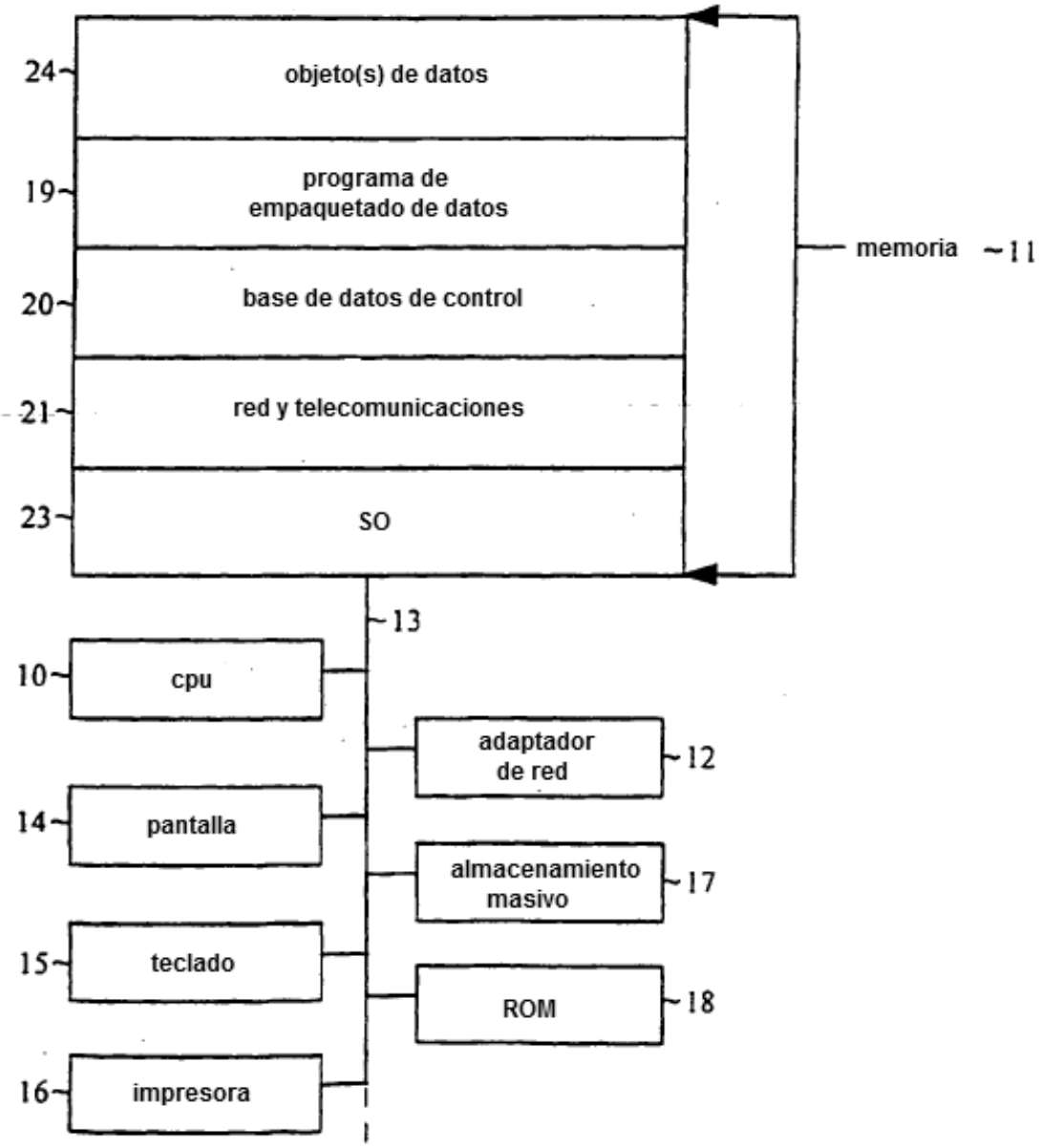

24
objeto(s) de datos
19
programa de empaquetado de datos
20
base de datos de control
21
red y telecomunicaciones
23
SO
memoria
11
13
10
cpu
adaptador de red
12
14
pantalla
almacenamiento masivo
17
15
teclado
ROM
18
16
impresora

Fig 3

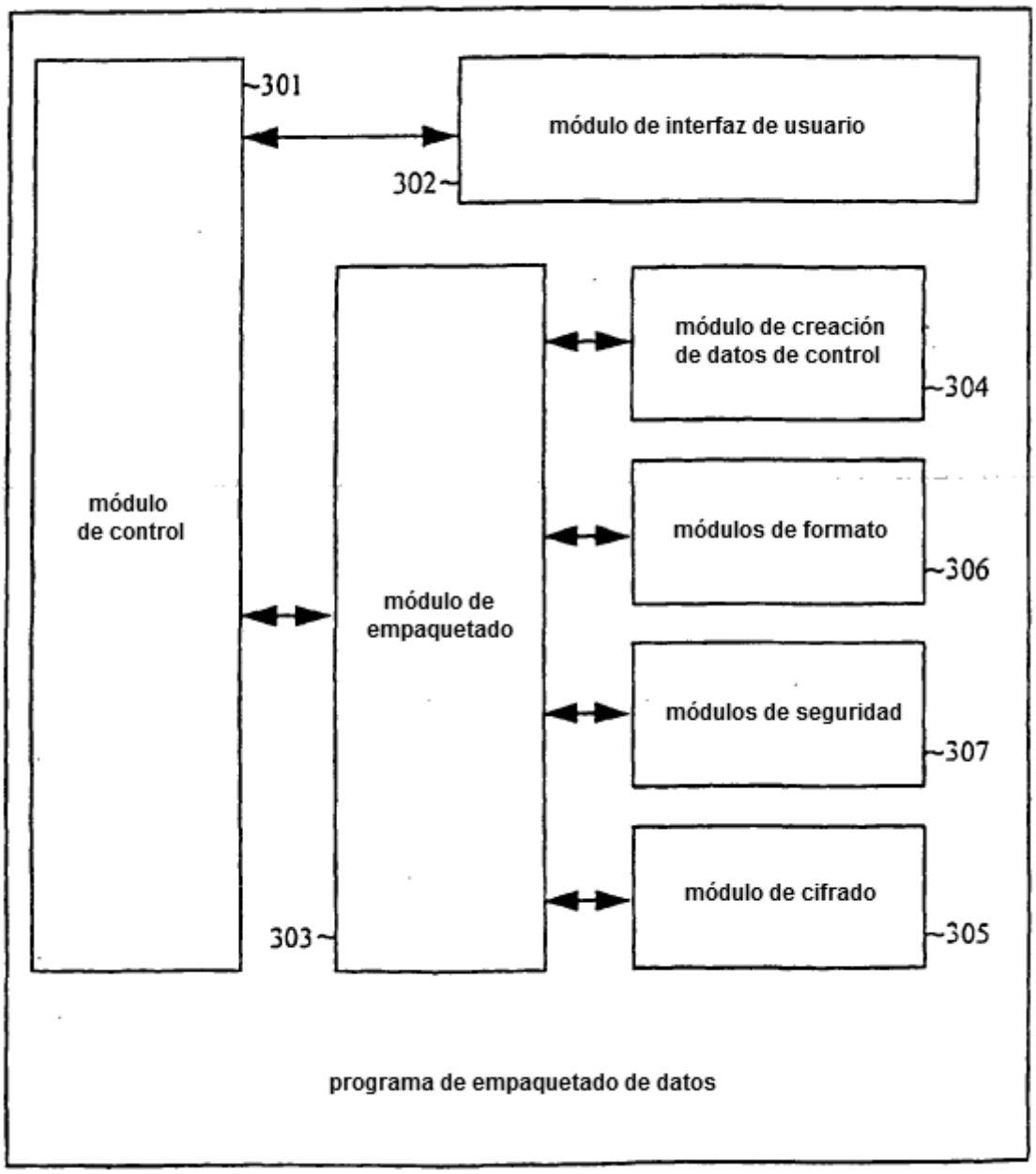

301
módulo de interfaz de usuario
302
módulo de creación de datos de control
304
módulo de control
módulos de formato
306
módulo de empaquetado
módulos de seguridad
307
módulo de cifrado
303
305
programa de empaquetado de datos

Fig 4

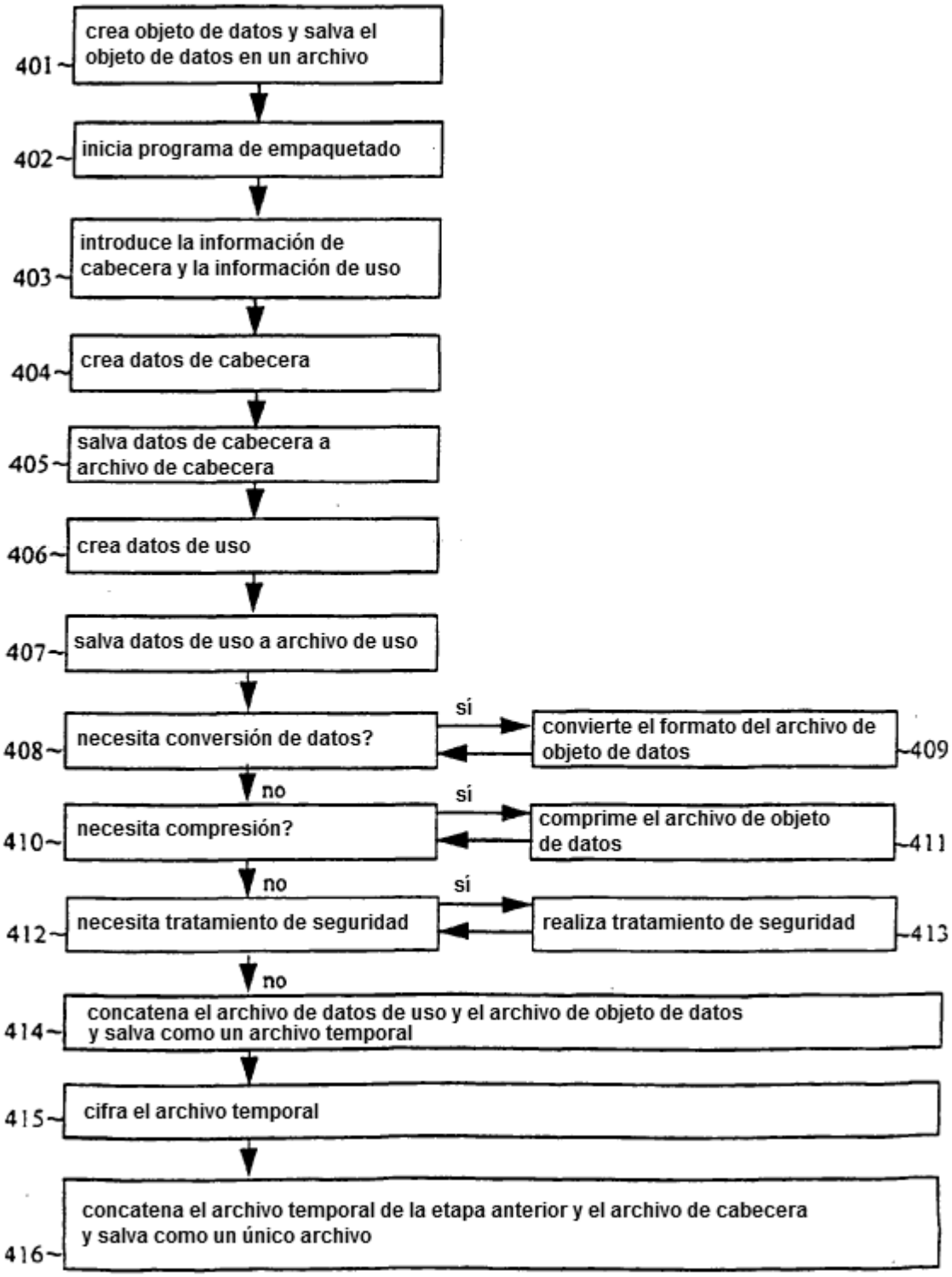

401
crea objeto de datos y salva el objeto de datos en un archivo
402
inicia programa de empaquetado
403
introduce la información de cabecera y la información de uso
404
crea datos de cabecera
405
salva datos de cabecera a archivo de cabecera
406
crea datos de uso
407
salva datos de uso a archivo de uso
408
necesita conversión de datos?
sí
409
convierte el formato del archivo de objeto de datos
no
410
necesita compresión?
sí
411
comprime el archivo de objeto de datos
no
412
necesita tratamiento de seguridad
sí
413
realiza tratamiento de seguridad
no
414
concatena el archivo de datos de uso y el archivo de objeto de datos y salva como un archivo temporal
415
cifra el archivo temporal
416
concatena el archivo temporal de la etapa anterior y el archivo de cabecera y salva como un único archivo

Fig 5

identificador de archivo	123456789
título	imagen
código de formato	a
código de seguridad	b

Fig 6

elemento de uso para el número de teléfono del autor	identificador	1
	tamaño	13
	datos	716 381 5356
... precio para un único uso	identificador	2
	tamaño	4
	datos	0,50
... precio para uso ilimitado	identificador	3
	tamaño	4
	datos	50,00
... código para tipo de uso aprobado	identificador	4
	tamaño	2
	datos	9
... código para número de usos aprobados	identificador	5
	tamaño	2
	datos	1

Fig 7

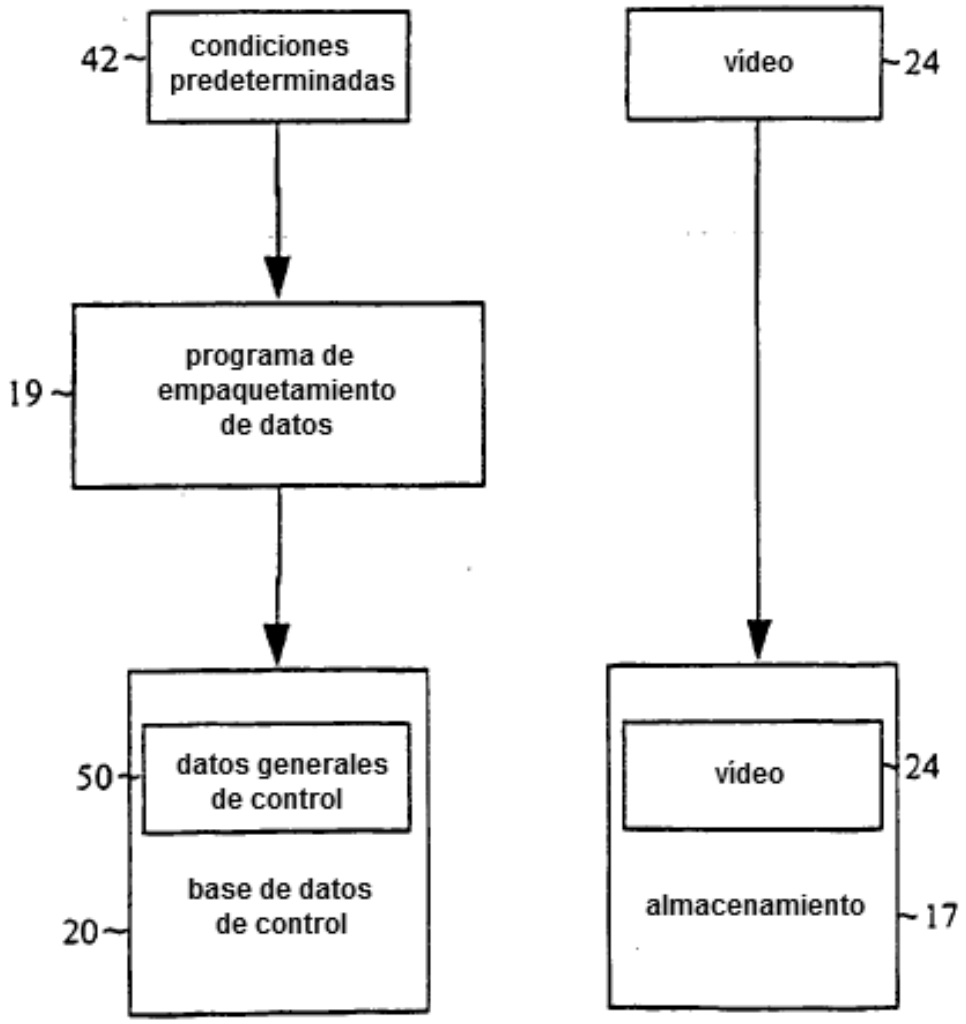

42
condiciones predeterminadas
vídeo
24
19
programa de empaquetamiento de datos
50
datos generales de control
vídeo
24
base de datos de control
20
almacenamiento
17

Fig 8a

cabecera	identificador de objeto	123456789
	código de formato	0010
	código de seguridad	0010
	número de elementos de uso	2
	tamaño de datos de uso	17
	tamaño de objeto de datos	273
	id del 1er elemento de uso	001
	tamaño del 1er elemento de uso	6
	datos del 1er elemento de uso	1
	id del 2º elemento de uso	002
	tamaño del 2º elemento de uso	3
	datos del 2º elemento de uso	

Fig 8b

cabecera	identificador de objeto	123456789
	código de formato	0010
	código de seguridad	0010
	número de elementos de uso	2
	tamaño de datos de uso	17
	tamaño de objeto de datos	273
	id del 1er elemento de uso	001
	tamaño del 1er elemento de uso	6
	datos del 1er elemento de uso	1
	id del 2º elemento de uso	002
	tamaño del 2º elemento de uso	3
	datos del 2º elemento de uso	2

Fig 9

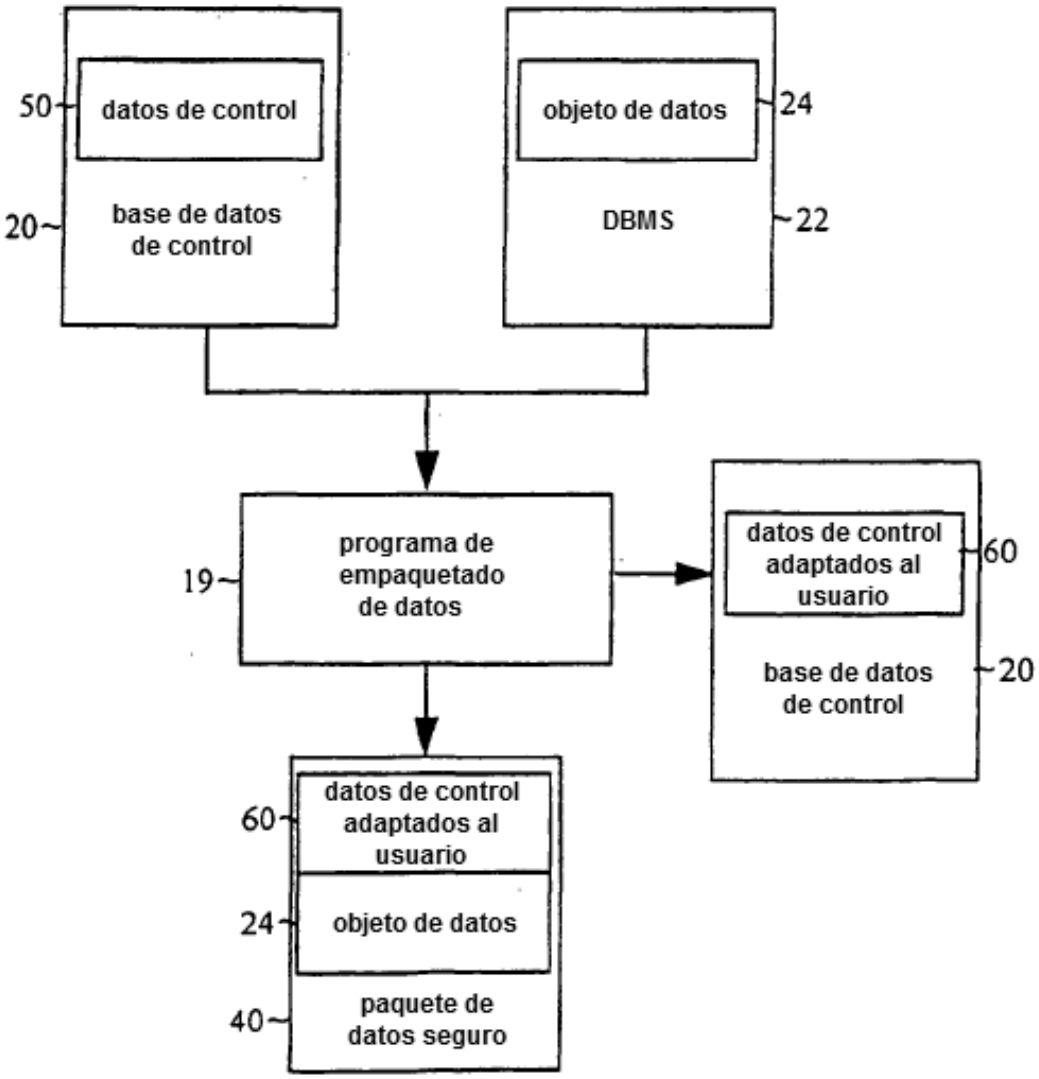

50
datos de control
base de datos de control
20
objeto de datos
24
DBMS
22
programa de empaquetado de datos
19
datos de control adaptados al usuario
60
base de datos de control
20
60
datos de control adaptados al usuario
24
objeto de datos
paquete de datos seguro
40

Fig 10

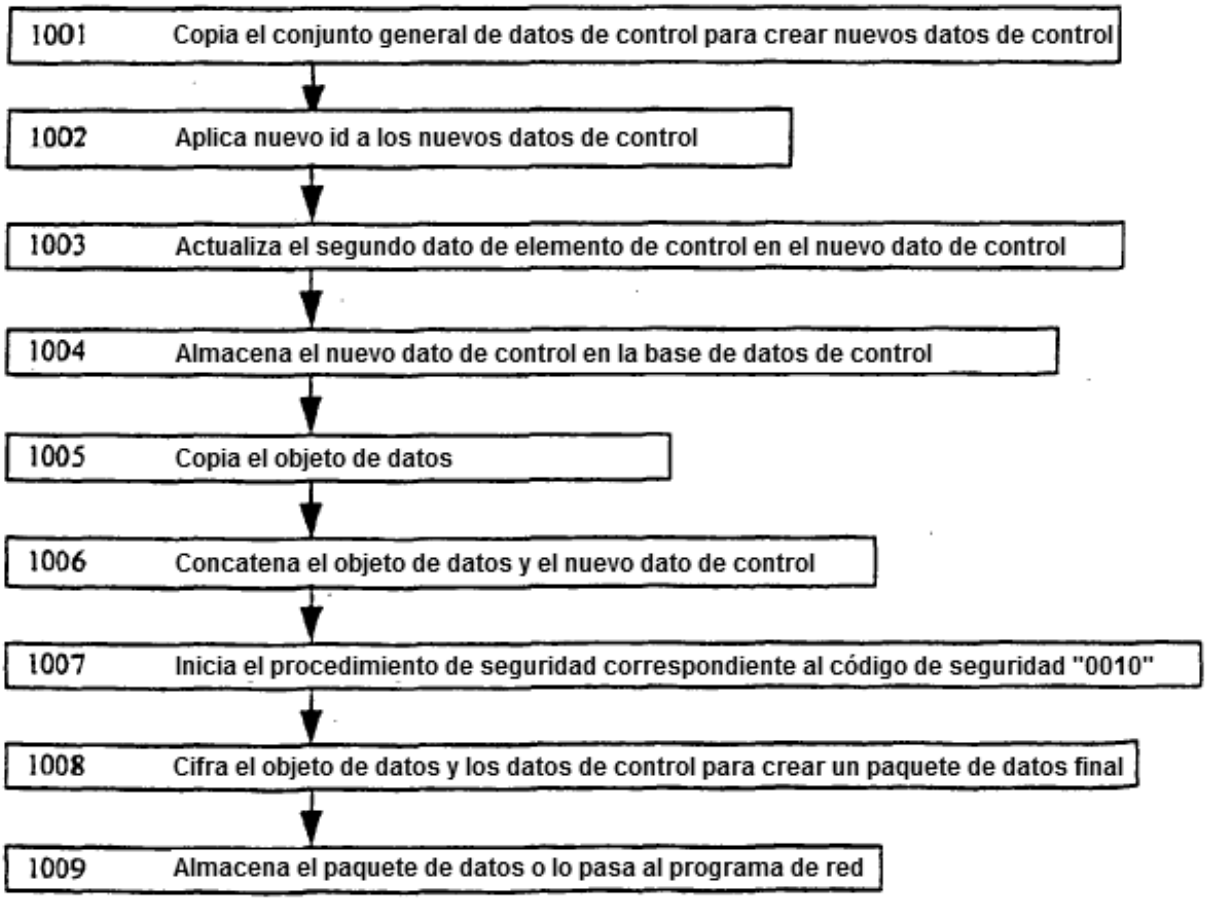
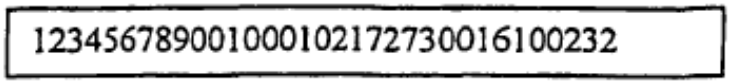

1001 Copia el conjunto general de datos de control para crear nuevos datos de control
1002 Aplica nuevo id a los nuevos datos de control
1003 Actualiza el segundo dato de elemento de control en el nuevo dato de control
1004 Almacena el nuevo dato de control en la base de datos de control
1005 Copia el objeto de datos
1006 Concatena el objeto de datos y el nuevo dato de control
1007 Inicia el procedimiento de seguridad correspondiente al código de seguridad "0010"
1008 Cifra el objeto de datos y los datos de control para crear un paquete de datos final
1009 Almacena el paquete de datos o lo pasa al programa de red

Fig 11

datos de control en memoria



archivo AVI en memoria

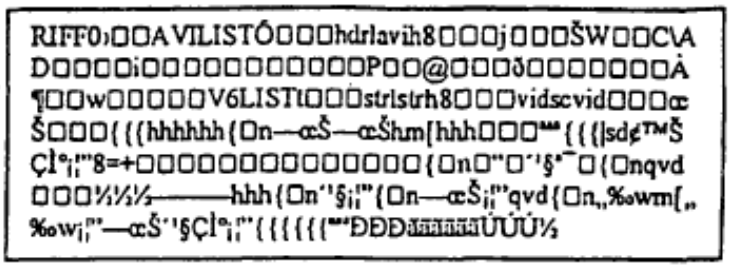


Fig 12a

datos de control y archivo AVI concatenados en memoria

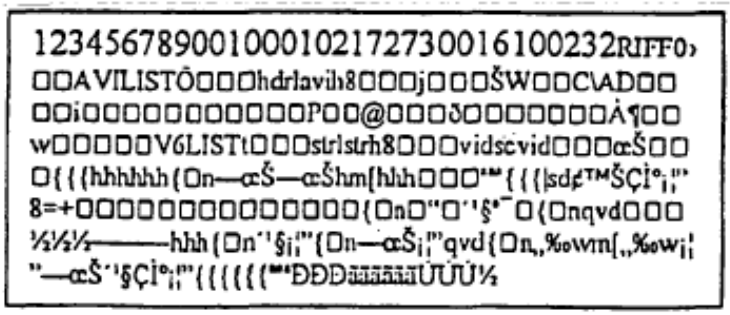


Fig 12b

datos de control y archivo AVI concatenados y cifrados en memoria

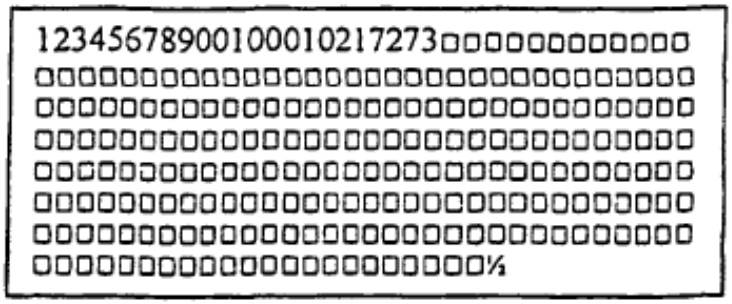


Fig 13

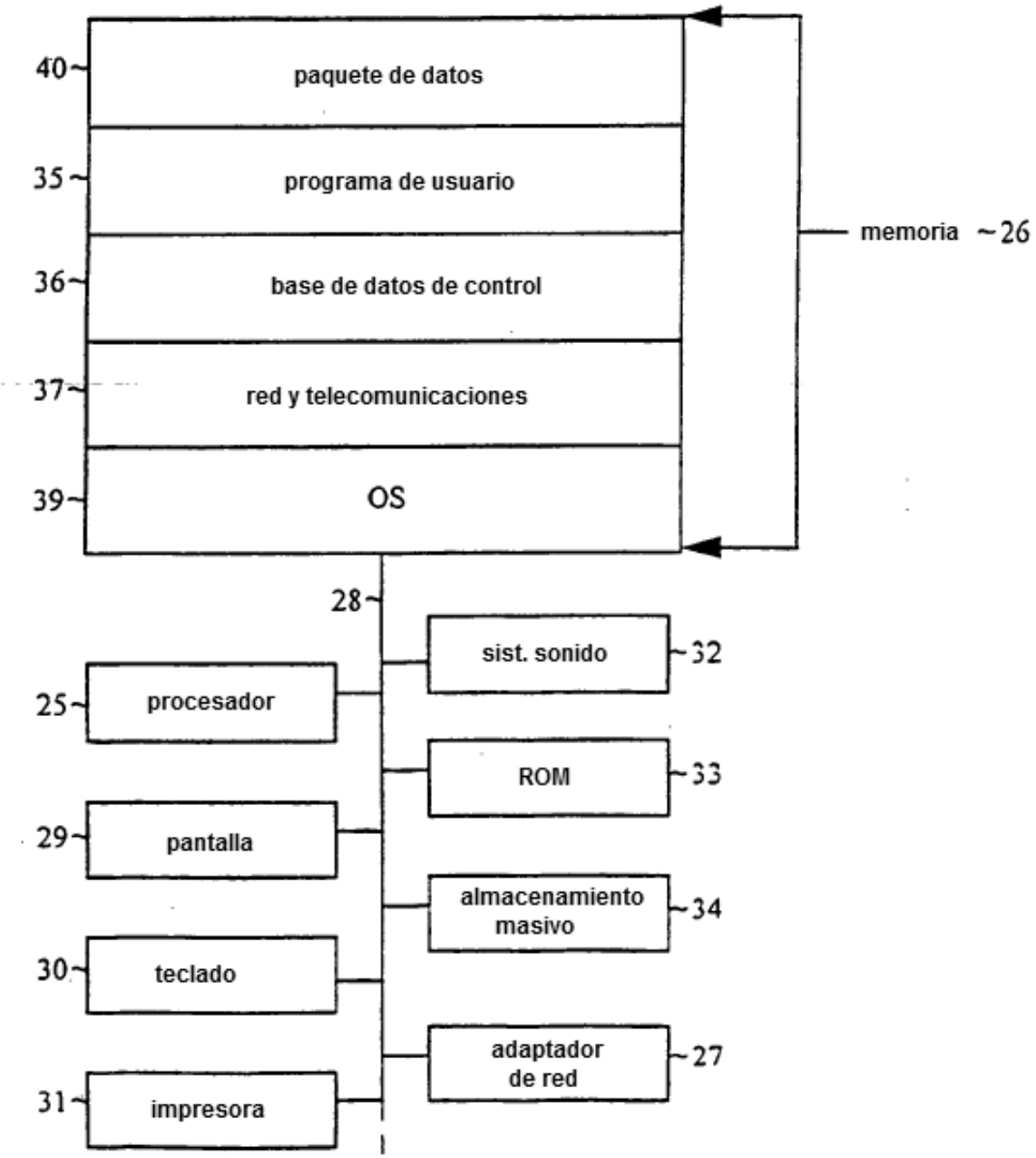

40
paquete de datos
35
programa de usuario
36
base de datos de control
37
red y telecomunicaciones
39
OS
memoria
26
28
sist. sonido
32
25
procesador
ROM
33
29
pantalla
almacenamiento masivo
34
30
teclado
adaptador de red
27
31
impresora

Fig 14

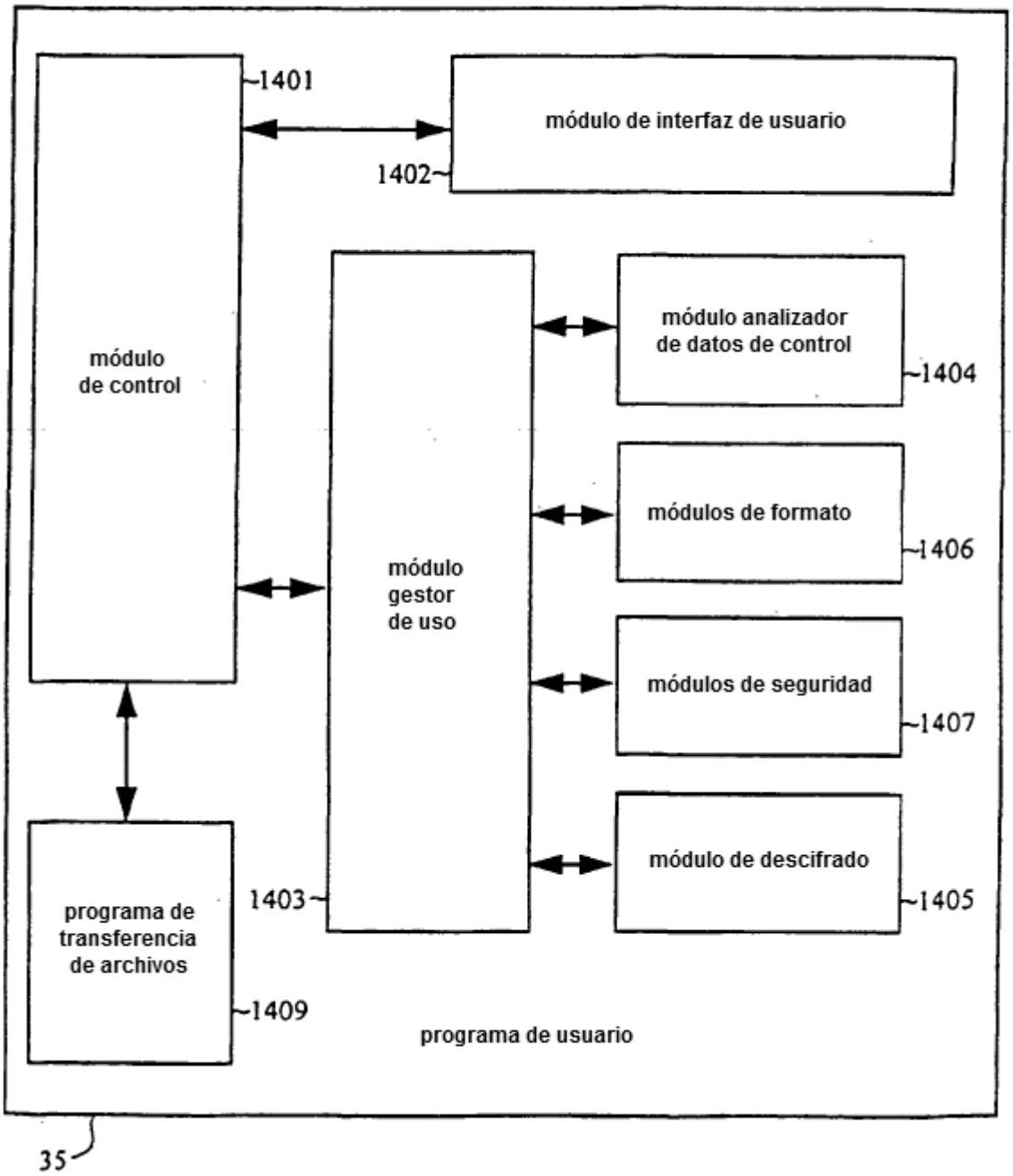

1401
módulo de interfaz de usuario
1402
módulo
de control
módulo analizador
de datos de control
1404
módulos de formato
1406
módulo
gestor
de uso
módulos de seguridad
1407
módulo de descifrado
1405
1403
programa de
transferencia
de archivos
1409
programa de usuario
35

Fig 15

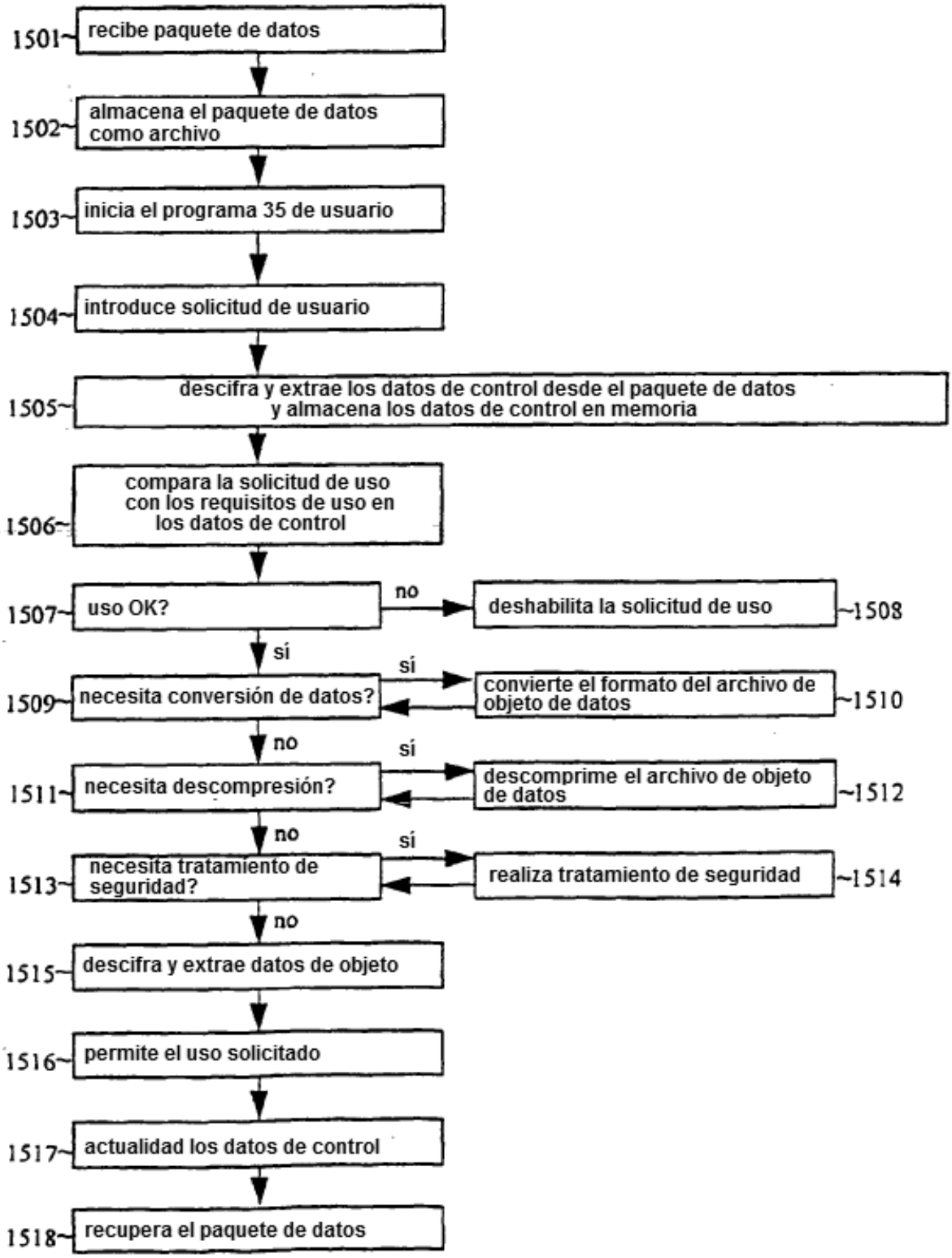

1501
recibe paquete de datos
1502
almacena el paquete de datos como archivo
1503
inicia el programa 35 de usuario
1504
introduce solicitud de usuario
1505
descifra y extrae los datos de control desde el paquete de datos y almacena los datos de control en memoria
1506
compara la solicitud de uso con los requisitos de uso en los datos de control
1507
uso OK?
no
deshabilita la solicitud de uso
1508
sí
1509
necesita conversión de datos?
sí
convierte el formato del archivo de objeto de datos
1510
no
1511
necesita descompresión?
sí
descomprime el archivo de objeto de datos
1512
no
1513
necesita tratamiento de seguridad?
sí
realiza tratamiento de seguridad
1514
no
1515
descifra y extrae datos de objeto
1516
permite el uso solicitado
1517
actualidad los datos de control
1518
recupera el paquete de datos

Fig 16

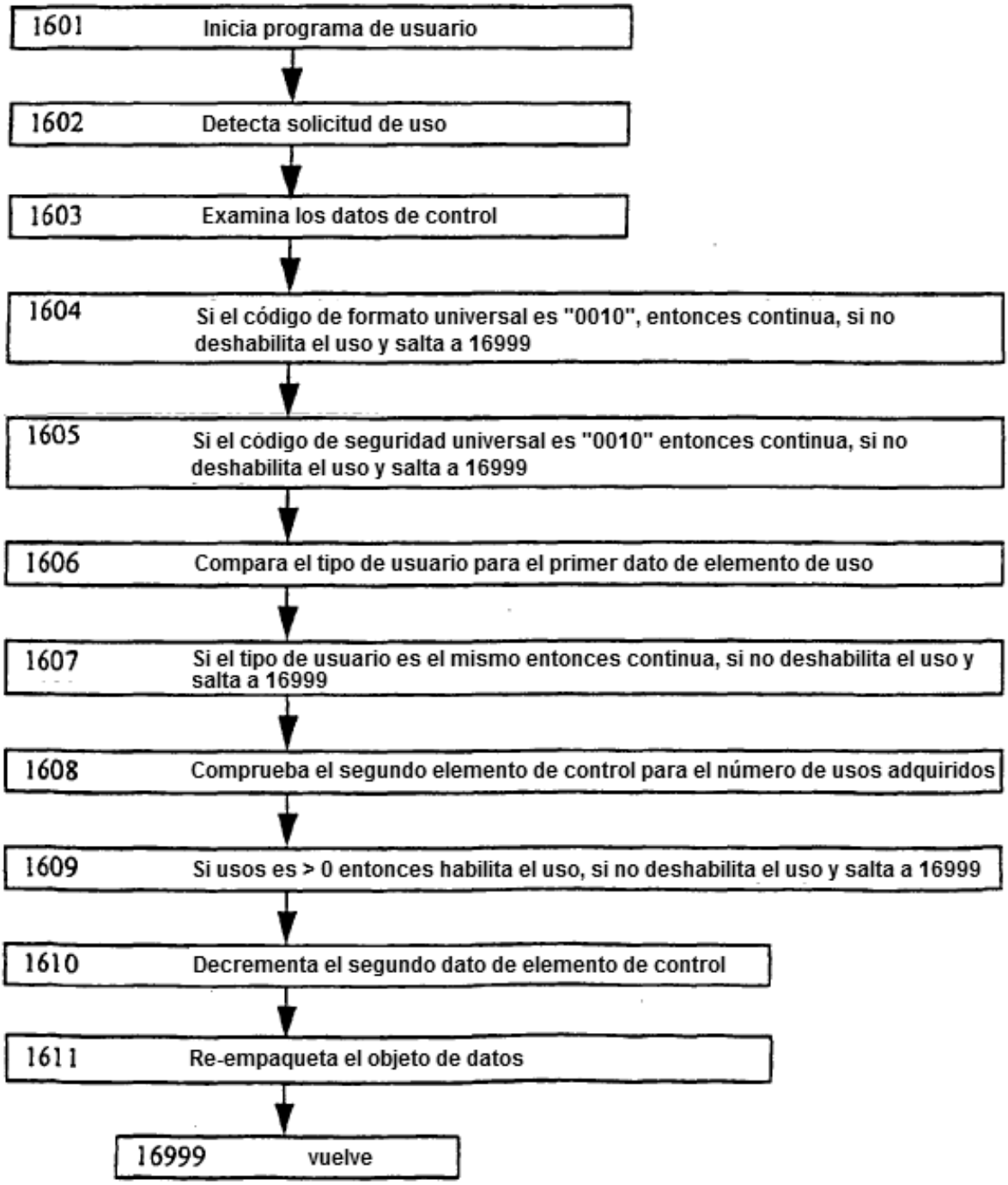
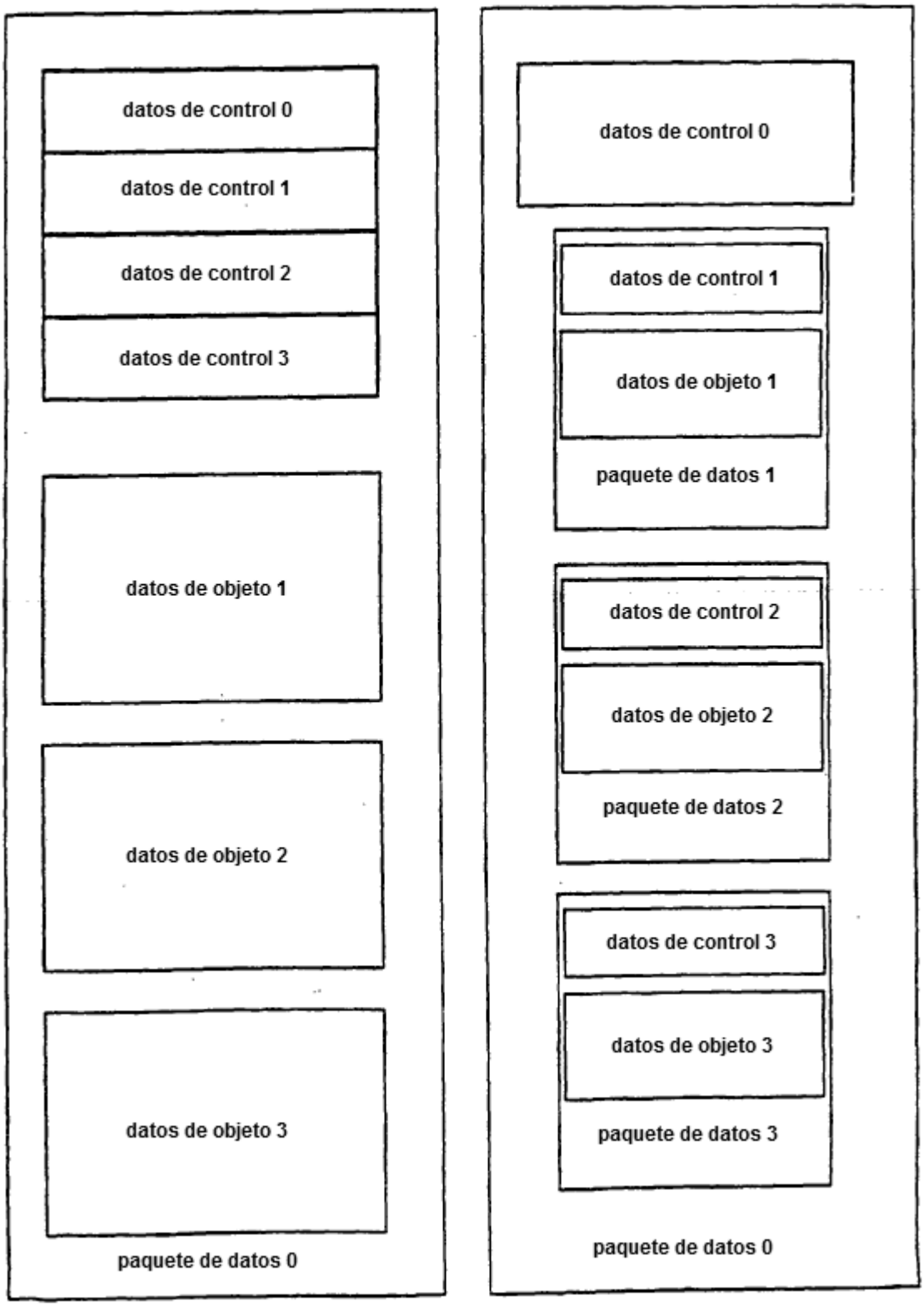

1601 Inicia programa de usuario
1602 Detecta solicitud de uso
1603 Examina los datos de control
1604 Si el código de formato universal es "0010", entonces continua, si no deshabilita el uso y salta a 16999
1605 Si el código de seguridad universal es "0010" entonces continua, si no deshabilita el uso y salta a 16999
1606 Compara el tipo de usuario para el primer dato de elemento de uso
1607 Si el tipo de usuario es el mismo entonces continua, si no deshabilita el uso y salta a 16999
1608 Comprueba el segundo elemento de control para el número de usos adquiridos
1609 Si usos es > 0 entonces habilita el uso, si no deshabilita el uso y salta a 16999
1610 Decrementa el segundo dato de elemento de control
1611 Re-empaqueta el objeto de datos
16999 vuelve

Fig 17


datos de control 0
datos de control 1
datos de control 2
datos de control 3
datos de objeto 1
datos de objeto 2
datos de objeto 3
paquete de datos 0
datos de control 0
datos de control 1
datos de objeto 1
paquete de datos 1
datos de control 2
datos de objeto 2
paquete de datos 2
datos de control 3
datos de objeto 3
paquete de datos 3
paquete de datos 0