(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 345 388**

(51) Int. Cl.:
***G06F 12/14*** (2006.01)
***G07F 7/10*** (2006.01)
***G06F 1/00*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04100546 .3**
(96) Fecha de presentación : **12.02.2004**
(97) Número de publicación de la solicitud: **1577782**
(97) Fecha de publicación de la solicitud: **21.09.2005**

(54) Título: **Método y sistema de almacenamiento de datos externo.**

(45) Fecha de publicación de la mención BOPI:
**22.09.2010**

(45) Fecha de la publicación del folleto de la patente:
**22.09.2010**

(73) Titular/es: **Irdeto Access B.V.**
**Jupiterstraat 42**
**2132 HD Hoofddorp, NL**

(72) Inventor/es: **Dekker, Gerard, Johan;**
**Bosscha, Albert-Jan y**
**Van de Ven, Antonius, Johannes,Petrus, Maria**

(74) Agente: **Tomás Gil, Tesifonte Enrique**

## DESCRIPCIÓN

Método y sistema de almacenamiento de datos externo.

### Antecedentes de la invención

La invención se refiere generalmente a métodos para almacenar datos externamente procesados por un dispositivo procesador. En particular, la invención se refiere a un método de almacenamiento de datos externo y a un método de interiorización de datos. La invención también se refiere a la aplicación de métodos de este tipo en un sistema multimedia y en un sistema y programa de ordenador para ejecutar tales métodos.

Ejemplos de un método que permite un almacenamiento de datos externo y de un método de almacenamiento de datos externo y un sistema adaptado para llevar a cabo tal método son conocidos, p. ej. de US 5 757 919. Esta publicación expone un método y un sistema para mantener la integridad y la confidencialidad de páginas mandadas a una unidad de memoria externa de un entorno físicamente seguro. Este entorno físicamente seguro contiene un procesador seguro acoplado por un bus a una memoria de acceso aleatorio. Un motor de control de integridad ejecuta un hash unidireccional de la transmisión de datos entre el entorno seguro y el entorno no seguro, particularmente una unidad de memoria externa. En una forma de realización, el procesador seguro está diseñado para utilizar una página de 1K. Un procesador host en el entorno no seguro trata las páginas del procesador seguro almacenadas en la memoria externa como bloques de datos de 1K. Si una página se identifica como necesaria, se determina si la página se encuentra dentro de la memoria segura. Si la página está presente, se obtiene un resultado de búsqueda y no se requiere ninguna otra acción. Si la página no está presente, ocurre un fallo de página. Cuando ocurre un fallo de página, se determina si hay espacio disponible en la memoria segura a la que se pueda aplicar la página requerida. Si no hay espacio disponible, entonces se selecciona una página para borrarla de la memoria. Pueden emplearse diferentes criterios de selección tales como aquellos que se utilizaron más recientemente.

El método y el sistema conocidos tienen la desventaja de que es difícil seleccionar la porción de datos a transferir al sistema de almacenamiento de datos secundario. Debido a que guardar y borrar páginas generalmente implica un tiempo de espera y los servicios de seguridad aumentan el tiempo de espera en caso de un fallo de página, esto enlentece el procesamiento de los registros activos.

Otro ejemplo de un método de almacenamiento de datos externo, un método de interiorización de datos, método para procesar registros en un sistema multimedia y un sistema adaptado para llevar a cabo tales métodos se describe en FR-A-2 803 471. Esta publicación expone un proceso de gestión de memoria en un televisor. El sistema de televisión comprende una televisión, medios de memoria local implantados en la televisión y medios de memoria externa asociados a la televisión, tales como una tarjeta de memoria o disquetera. El sistema comprende un programa de ordenador comprendiendo una pluralidad de módulos ejecutables. Un primer módulo recibe y analiza cada solicitud para memorizar información. Si las características de los medios de memoria no permiten el almacenamiento de información nueva, el primer módulo activa un segundo módulo. El segundo módulo libera espacio de memoria mientras que respeta el criterio de uso de la información almacenada. El primer y el segundo módulo usan una serie de procedimientos simples para optimizar el almacenamiento de información. Estos procedimientos realizan, por ejemplo, la eliminación de datos de un primer medio de memoria a un segundo medio de memoria.

Un problema de este sistema conocido y método es que estos no permiten el tratamiento de parte o de la totalidad del registro una vez se ha externalizado. Si esto fuera a ocurrir y la porción de datos se fuera a transferir a la televisión en una etapa posterior, el conjunto completo de datos del registro no sería idéntico al conjunto completo de datos como se procesó anteriormente por la aplicación en el aparato de televisión antes de la exteriorización.

EP-A2-0 856 818 se refiere a una tarjeta IC conteniendo un módulo de circuito integrado comprendiendo una unidad procesadora central (CPU) y memoria interna. La CPU forma un medio de acceso de la tarjeta IC. El medio de acceso de la memoria interna constituye un sistema operativo y es capaz de procesar un acceso de la tarjeta IC a un medio de aceptación de la tarjeta IC externa. La tarjeta IC dispone de una memoria externa montada sobre la superficie del cuerpo de la tarjeta IC. La CPU está normalmente provista de un ROM del programa que crea dentro el medio de acceso de la memoria interna y un medio de acceso de la memoria externa. Los medios en realidad se establecen como programas. La tarjeta IC teniendo una función de seguridad está comprendida de la memoria externa, un medio de guardado de direcciones para guardar direcciones de los ficheros almacenados en la memoria externa, un medio de información de memoria de gestión criptográfica para almacenar la información de gestión criptográfica usada para cifrar datos y para descifrar los datos cifrados, un medio de procesamiento de escritura, un primer medio de procesamiento de lectura y un segundo medio de procesamiento de lectura. Los medios de procesamiento de escritura y de lectura son funciones de la CPU.

Al escribir datos en la memoria externa, un comando de escritura dado y los correspondientes datos de escritura se introducen en la tarjeta IC. Al leer datos desde la memoria externa, un primer comando de lectura y el número de fichero correspondiente se introducen en la tarjeta IC.

WO 00/26866 expone un método para operar un dispositivo portátil IC con una memoria para almacenar objetos de datos. El método consiste en almacenar objetos de datos que de otra manera serían almacenados normalmente en la tarjeta en un medio de almacenamiento remoto, y clasificar en la tarjeta de una manera segura especial la información

necesaria para marcar y recuperar los objetos de datos. El sistema puede diseñarse para detectar una condición predeterminada relacionada con la memoria de la tarjeta, y si se detecta la condición, para aplicar el método de clasificación en varios de los objetos de datos almacenados en la memoria de la tarjeta. La condición puede ser por ejemplo una saturación de la memoria de la tarjeta, en cuyo caso el método se utiliza para liberar la memoria de la tarjeta para proporcionar espacio para otros objetos de datos.

**Resumen de la invención**

La invención proporciona un método de almacenamiento de datos externo, un método para la interiorización de un registro, un dispositivo procesador primario y medios de programas de ordenador más eficaces en cuanto al número de transferencias de datos a y desde el sistema de almacenamiento secundario.

Esto se consigue mediante un método de almacenamiento de datos externo tal y como se define en la reivindicación 1.

Cuando el método se aplica, el control sobre el almacenamiento externo de datos pertenecientes a los registros se transfiere al programa de aplicación que está usando los datos en ese momento. La llamada puede ser a una interfaz de programación de aplicaciones adaptada para llevar a cabo el método para permitir el almacenamiento externo de datos según la invención. De forma alternativa, el método se puede realizar directamente mediante un programa de aplicación que funciona en el dispositivo procesador primario. Así confiere la ventaja de permitir que el programa de aplicación determine si un registro se exterioriza o no. Así, el programa de aplicación puede prevenir que una porción de datos de un registro que se va a procesar en un breve periodo de tiempo se transfiera al dispositivo de almacenamiento secundario. La ejecución del programa de aplicación se acelera así, ya que la latencia asociada a la exteriorización del registro y la posterior recuperación de la porción de datos del sistema de almacenamiento secundario cuando ésta se va a volver a modificar, se evita.

Preferiblemente, el método incluye transferir una sección de datos incluyendo los datos correspondientes a al menos una parte asociada de sólo una porción de datos de un registro.

Así cada sección de datos transferida al sistema de almacenamiento secundario para el almacenamiento incluye datos correspondientes a una parte asociada de sólo una porción de datos. En casos donde más de un registro se va a exteriorizar, esto excluye almacenar secciones de datos con una sub-sección correspondiente a datos de un registro y una sub-sección correspondiente a datos de otro registro. En otras palabras, los datos correspondientes a datos de un registro se almacenan siempre en una sección de datos diferente de los datos correspondientes a los datos de otro registro. La forma de realización tiene la ventaja de eliminar la transferencia de datos innecesaria a y particularmente desde el sistema de almacenamiento secundario.

En una forma de realización preferida, la porción de datos se divide en una pluralidad de partes y donde una pluralidad de secciones de datos, cada una incluyendo datos correspondientes a una de las partes asociadas de la pluralidad de partes, se transfiere al sistema de almacenamiento de datos secundario para el almacenamiento.

Esta forma de realización tiene la ventaja de permitir que la exteriorización se adapte al tamaño de la memoria principal disponible para el dispositivo procesador primario y/o a las características de la interfaz para el sistema de almacenamiento secundario, tales como la anchura de un ducto de datos.

En una forma de realización preferida, los datos correspondientes a una parte asociada se generan, al menos parcialmente, encriptando la parte asociada de la porción de datos.

Debido a que las secciones de datos transferidas al sistema de almacenamiento secundario para el almacenamiento están al menos parcialmente encriptadas, sólo la unidad de almacenamiento de datos primaria y el procesador del dispositivo de procesamiento de datos primario deben ocultarse en un entorno seguro para mantener una seguridad global absoluta de los datos. Debido a que el dispositivo procesador primario sólo necesita tener una unidad de almacenamiento primaria con una capacidad de memoria limitada, gracias a la posibilidad de almacenar datos externamente, es más barato y más fácil proporcionar tal entorno seguro.

Preferiblemente, el método incluye calcular un valor de autenticación para cada parte de la porción de datos e incluir datos reflejando el valor de autenticación en la sección de datos que incluye datos correspondientes a esa parte.

Así, la integridad de los datos almacenados externamente se puede verificar.

Una variante preferida de esta forma de realización incluye calcular el valor de autenticación para al menos una parte de la porción de datos usando información derivada de otra parte como entrada.

Así, dónde la porción de datos se divide en partes y se almacena externamente en secciones de datos diferentes, la integridad del conjunto entero de secciones de datos se puede verificar.

Preferiblemente, el método incluye almacenar un objeto de datos de referencia en una unidad de almacenamiento de datos del dispositivo primario para cada registro exteriorizado, incluyendo un identificador único, donde los datos

reflejando el identificador único se incluyen en cada sección de datos que incluye datos correspondientes a una parte de la porción de datos del registro.

Así, se facilita la recuperación de diferentes secciones de datos conteniendo datos correspondientes a la porción de datos almacenada externamente.

Preferiblemente, el método de la invención incluye almacenar información reflejando un conteo de versiones para el registro externalizado e incrementar el conteo de versiones antes de exteriorizar el registro.

De esta manera es posible seguir los movimientos del número de veces que el registro se ha exteriorizado. Esto habilita la sincronización de los datos del registro que está almacenado en la unidad de almacenamiento primaria y la porción de datos que está almacenada externamente.

Según otro aspecto de la invención, se proporciona un método para la interiorización de un registro tal y como se define en la reivindicación 9.

Así, el programa de aplicación configurado para usar los datos de un registro determina que una porción de datos de un registro se va a transferir al dispositivo procesador primario del sistema de almacenamiento secundario. El dispositivo procesador primario puede ser igual que el dispositivo procesador primario involucrado en la transferencia de la porción de datos al sistema de almacenamiento secundario, o puede ser diferente. Así, el método tiene la ventaja de permitir que se compartan los datos de un registro.

Una forma de realización preferida de la invención incluye recibir al menos una sección de datos incluyendo datos correspondientes a al menos una parte asociada de una porción de datos del sistema de almacenamiento secundario.

Así, la sección de datos incluye datos correspondientes a una parte asociada de una porción de datos de un registro. No es necesario separar los datos de un registro de los de otro registro, ni transferir los datos de otro registro de forma innecesaria con datos de un registro cuyo programa de aplicación ha determinado como necesario.

Preferiblemente, el método incluye recuperar un identificador único para el registro a partir de un objeto de referencia almacenado en una unidad de almacenamiento de datos del dispositivo procesador primario, donde las secciones de datos se almacenan en el sistema de almacenamiento de datos secundario con información reflejando el único identificador y se reciben en respuesta a un mensaje de interiorización incluyendo el reflejo de la información del único identificador.

Así, el dispositivo procesador primario permanece consciente de la existencia del registro y tiene un mecanismo para acceder a los datos de éste, incluso cuando los datos no están almacenado en la unidad de almacenamiento de datos primaria.

Una forma de realización preferida de la invención, donde la porción de datos comprende una pluralidad de partes, incluye recibir varias secciones de datos, cada una incluyendo datos correspondientes a una parte asociada de la pluralidad de partes.

Así, esta forma de realización del método se puede ejecutar en un dispositivo procesador primario con capacidad de procesamiento limitada, p. ej. una memoria principal limitada, mientras que la parte de la porción de datos del registro que se está internalizando se puede procesar y cargar en la unidad de almacenamiento de datos primaria consecutivamente. Esta forma de realización también está adaptada para tener en cuenta cualquier limitación para la capacidad de una interfaz para el sistema de almacenamiento de datos secundario.

Una forma de realización preferida incluye recibir al menos una sección de datos incluyendo un valor de autenticación, recuperar una porción secreta de información almacenada en el dispositivo procesador primario, calcular un valor de autenticación de verificación para cada sección de datos de al menos parte de los datos correspondientes a al menos una parte asociada de la porción de datos, usando la porción secreta de información, y comparar el valor de autenticación de verificación y el valor de autenticación para cada sección de datos.

Así, se puede determinar si los datos incluidos en las secciones de datos recibidos son auténticos. Debido a que se calcula el valor de autenticación de verificación, no hay ninguna necesidad de depositarlo en el dispositivo procesador primario, en particular en la unidad de almacenamiento de datos primaria.

Preferiblemente, el método incluye recibir una sección de datos incluyendo información reflejando un conteo de versiones para el registro externalizado y comparar el conteo de versiones con un conteo de versiones de referencia.

Esto posibilita que el dispositivo procesador primario verifique que los datos recuperados son los datos pertenecientes a una versión del registro que está prevista. Es particularmente útil si otros dispositivos de procesamiento primarios pueden haber tenido acceso a la porción de datos almacenada externamente.

Una ventaja se obtiene a través de la aplicación de cualquiera de los métodos mencionados arriba en un método de procesamiento de registros en un sistema multimedia, adaptado para proporcionar acceso por lo menos una porción

consecutiva de contenido digital formando un evento e incluyendo un sub-sistema de acceso condicional dispuesto para controlar el acceso al evento conforme a la información contenida en al menos un registro, donde el sistema multimedia incluye un dispositivo procesador primario seguro, con un procesador y una unidad de almacenamiento de datos primaria, adaptados para activar al menos un programa de aplicación para procesar registros activos en el procesador cuando un evento se está accediendo y configurando para alamcenar datos pertenecientes a un registro activo en la unidad de almacenamiento de datos primaria; y un sistema de almacenamiento de datos secundario, accesible al dispositivo procesador primario.

En el contexto de la presente invención, el término 'seguro' significa que el dispositivo procesador primario está equipado con medios para resistir ataques invasivos y no invasivos en los datos almacenados y/o procesados por él, lo cual significa que puede ser hardware o software implementado o estar implementado por una combinación de ambos. Debido a que el coste y el esfuerzo involucrados en hacer el dispositivo procesador primario resistente a manipulación aumentan con su capacidad, es decir el almacenamiento y/o la capacidad de procesamiento, se prefiere limitar el tamaño, en particular el tamaño de la unidad de almacenamiento de datos primaria. La invención permite hacer esto mientras que retiene la capacidad de acceso a un gran número de registros diferentes, como parte o totalidad de los datos pertenecientes a los registros que se pueden almacenar externamente en el sistema de almacenamiento secundario en una manera ventajosa.

Según otro aspecto de la invención, se proporciona un dispositivo procesador primario, con un procesador y una unidad de almacenamiento de datos primaria, adaptado para procesar registros activos en el procesador, configurado para almacenar datos de un registro activo en la unidad de almacenamiento de datos primaria, y adaptado para ejecutar cualquiera de los métodos expuestos arriba según la invención.

Según otro aspecto de la invención se proporcionan medios de programas de ordenador los cuales, al activarse por un dispositivo procesador primario con un procesador y una unidad de almacenamiento de datos primaria, permiten que el dispositivo procesador primario ejecute cualquiera de los métodos expuestos arriba según la invención.

La invención se describirá ahora con más detalle con referencia a los dibujos anexos, de los cuales

**Breve descripción de los dibujos**

Fig. 1 es una vista de conjunto muy esquemática de un tipo de sistema para el cual la invención está destinada.

Fig. 2 es un diagrama esquemático de una base de datos mantenida por el dispositivo procesador primario en una variante de la invención.

Fig. 3 es un diagrama esquemático de una base de datos almacenada en el sistema de almacenamiento secundario en la variante de la Fig. 3.

Fig. 4 es un diagrama de flujos que ilustra la creación de un registro.

Fig. 5 es un diagrama de flujos que ilustra la modificación del registro por el dispositivo procesador primario.

Fig. 6 es un diagrama de flujos que ilustra diferentes fases en la exteriorización de un registro.

Fig. 7 muestra un ejemplo de un sistema multimedia en el cual se ha implementado la invención.

Fig. 8 muestra un ejemplo de la arquitectura básica del dispositivo procesador primario mostrado en la Fig. 1.

**Descripción específica**

Para explicar los principios generales del método de almacenamiento de datos externo según la invención, la Fig. 1 muestra un ejemplo simplificado de un sistema en el cual éste se puede aplicar. Un ejemplo más específico se ilustrará abajo con referencia a las Figs. 7 y 8.

En la Fig. 1 un primer dispositivo procesador 1 comprende una (CPU) de la unidad de procesamiento central 2, memoria principal 3 y un dispositivo de almacenamiento de la masa primaria 4. El primer dispositivo procesador 1 puede, por ejemplo, implementarse como un servidor (p. ej. un servidor de la base de datos), un ordenador personal, asistente digital personal, dispositivo procesador insertado, teléfono móvil, etc. en resumidas cuentas, cualquier dispositivo procesador de datos con un procesador, una unidad de almacenamiento de datos y medios para acceder a una unidad de almacenamiento de datos secundaria es adecuado para la implementación de la invención. Dependiendo de la implementación, la memoria principal 3 puede estar integrada en un único chip con la CPU 2.

En el ejemplo a describir aquí, el método según la invención se utiliza para sacar el mejor partido de la capacidad limitada del dispositivo de almacenamiento de masa primaria 4, transfiriendo temporalmente datos del dispositivo de almacenamiento de masa primaria 4 a un sistema de almacenamiento secundario. No obstante, el método podría igualmente bien aplicarse para hacer mejor uso de la capacidad de la memoria principal 3 o de una memoria caché (no mostrada) en la CPU 2. Así, el término unidad de almacenamiento de datos primaria como se utiliza en este caso puede

referirse a ambos medios de almacenamiento de datos volátil y no volátil, incluyendo dispositivos de almacenamiento ópticos, magnético y de estado sólido.

En la Fig. 1, el primer dispositivo procesador 1 se conecta a un sistema de almacenamiento de datos secundario, formado por un segundo dispositivo procesador 5. La conexión se hace mediante un enlace de datos 6. El segundo dispositivo procesador 5 también comprende una unidad de procesamiento central (CPU) 7 con la memoria principal 8 y el primer y el segundo dispositivos de almacenamiento de masa secundarios 9 e 10, respectivamente. En formas de realización básicas de la invención, no es un requisito necesario que el segundo dispositivo procesador comprenda la CPU 7, aunque algún tipo de microprocesador para dirigir datos a los dispositivos de almacenamiento de masa secundaria estará presente si el sistema de almacenamiento secundario se implementa como un dispositivo externo tal como el segundo dispositivo procesador 5. En su forma de realización más simple, la invención podría simplemente sacar el mejor partido de la capacidad limitada del dispositivo de almacenamiento de masa primario 5 transfiriendo temporalmente datos a un segundo dispositivo de almacenamiento de masa dentro del primer dispositivo procesador 1.

En la forma de realización preferida, no obstante, se hace uso de un dispositivo externo, debido a que el método de la invención se implementa en un sistema en el que el dispositivo procesador primario se asegura más contra ataques de piratería informática que el dispositivo procesador secundario. En sistemas de este tipo, el método según la invención es particularmente útil en tanto en cuanto proporciona un mecanismo mediante el cual la capacidad y/o el tamaño del dispositivo procesador primario se puede mantener pequeño, haciéndolo así más fácil y más barato de proteger.

El enlace de datos 6 puede ser un enlace de red, por ejemplo un Ethernet, enlace IEEE 1394 (FireWire), o puede ser un enlace bus de datos, por ejemplo usando un USB, SCSI, RS-232, Bluetooth o enlace de tipo similar. Dependiendo del tipo de enlace usado y la capacidad de procesamiento necesaria para procesar mensajes pertenecientes al protocolo, un simple controlador se puede sustituir para la CPU 7 del segundo dispositivo procesador.

El primer dispositivo procesador 1 se adapta para activar uno o más programas de aplicación, los cuales se ejecutan mediante la CPU 2. Al menos un programa de aplicación se configura para procesar registros. Para este fin, un registro se entiende como una colección de unidades de datos dispuestas para su procesamiento mediante el programa de aplicación. La disposición de los datos se prescribe por el programa de aplicación que lo procesa. La invención encierra ambos registros de longitud fija y de longitud variable. Según la invención, los registros a procesar por el programa de aplicación ejecutado en la CPU 2, se hacen activos. Los registros activos, es decir todos los datos pertenecientes a registros hechos activos por programas de aplicación que se están ejecutando en el primer dispositivo procesador 1 en cualquier instante, se almacenan en el dispositivo de almacenamiento de masa primario 4, al menos durante tanto tiempo como los registros estén activos. Esto no excluye que (posiblemente ya no actuales) copias de parte o de la totalidad de los datos se almacenen también en otro lugar, por ejemplo en uno de los dispositivos de almacenamiento de masa secundarios 9,10.

Los programas de aplicación según la invención se configuran para decidir de manera autónoma si se almacena parte o la totalidad de los datos externamente, es decir en un dispositivo de almacenamiento diferente del dispositivo de almacenamiento de masa primario 4. Las reglas según las cuales se han tomado tales decisiones pueden variar. Por ejemplo, parte o la totalidad de los datos pueden salvarse. No obstante, la invención se usa preferiblemente para exteriorizar un registro porque una parte grande de los datos del registro se puede eliminar del dispositivo de almacenamiento de masa primaria 4 para liberar espacio. Esta parte, o los datos que permitir su recuperación, es decir datos correspondientes a esta parte, se transfere para uno de los dispositivos del almacenamiento de la masa secundaria 9,10 para almacenamiento y más tarde recuperación mediante procesos denominadas en este caso como exteriorización y interiorización, respectivamente.

Al determinar que un registro se va a exteriorizar, el programa de aplicación hace una llamada a una interfaz, dispuesta para transferir una porción de datos del registro al segundo dispositivo procesador 5. Una interfaz se define aquí como la disposición física y lógica que soporta el anexo al sistema de almacenamiento secundario. Preferiblemente, otro programa de aplicación o sistema operativo se instala en el primer dispositivo procesador 1, el cual soporta una interfaz del programa de aplicación, a la cual el el programa de aplicación que procesa el registro a exteriorizar puede hacer una llamada. Así, los desabolladores de programas de aplicación para el primer dispositivo procesador 1 no necdeben preocuparse por el mecanismo exacto de la exteriorización de registros. Sin embargo, formas de realización en las cuales parte o la totalidad la lógica para la exteriorización del registro se comprende en el programa de aplicación no se excluyen del alcance de la presente invención. En formas de realización de este tipo, la interfaz referida es en sentido amplio la interfaz física, es decir el mecanismo para transferir datos sobre el enlace de datos 6 al segundo dispositivo procesador 5.

Se observa que en la presente invención, el programa de aplicación funciona en el primer dispositivo procesador 1 y procesar el registro hace la llamada a la interfaz para exteriorizar el registro. No obstante, otra aplicación, usando datos del registro, proporcionados a ésta por la aplicación que procesa el registro en el primer dispositivo procesador, también puede hacer la llamada y concluir además el procesamiento del registro a través del programa de aplicación ejecutado en el primer dispositivo procesador 1. Esta otra aplicación puede incluso ejecutarse en un dispositivo procesador separado conectado al primer dispositivo procesador 1, incluso en el segundo dispositivo procesador 5.

Para permitir la posterior interiorización del registro, una base de datos primaria (Fig. 2) se almacena en una unidad de almacenamiento de datos primaria del dispositivo procesador primario 1. Este es, preferiblemente, el dispositivo de almacenamiento en masa primario 4, pero puede ser otra unidad de almacenamiento de datos, p. ej. la memoria principal 3, o alguna otra unidad de memoria volátil o no volátil. Nótese que la unidad de almacenamiento de datos primaria en la cual el primer dispositivo procesador 1 almacena la base de datos primaria también puede ser un dispositivo periférico, pero preferiblemente es un dispositivo interno para un acceso más rápido a la base de datos primaria. En cualquier caso, preferiblemente se incluye en un entorno seguro compartido con el primer dispositivo procesador 1.

La composición de una tabla de base de datos primaria 11 en la base de datos primaria se ilustra en la Fig. 2. Nótese que la tabla es un ejemplo de una implementación de la invención. La estructura de los datos exacta no es importante para la invención, mientras que haya al menos un objeto de datos de referencia para cada registro que se ha exteriorizado. En este ejemplo, hay un registro de la base de datos primaria 12a-12e, correspondiente a una fila en la tabla de base de datos primaria 11, para cada registro exteriorizado. Cada registro de la base de datos primaria 12 comprende un campo en una columna de índice 13, conteniendo una clave única o número de índice usado para acceder al registro de la base de datos primaria 12. El valor en la columna de índice 13 es único para cada registro exteriorizado. En una columna del número de versión 14 de la tabla de base de datos primaria 11, un número de la versión se almacena para cada registro externalizado. El número de la versión puede ser un simple contador, o puede ser cualquier otro tipo de información que refleje un conteo de versiones para el registro asociado exteriorizado. Por ejemplo, donde un registro comprende varios campos de los cuales cada uno puede tener un número finito de valores, la información en la columna del número de versión 14 puede ser información que identifica de manera única uno de los números finitos de permutaciones posibles de los valores en los campos del registro exteriorizado. Otros tipos de información reflejando un conteo de versiones son concebibles.

En el ejemplo presente, el segundo dispositivo procesador 5 mantiene una tabla de registro de extensión 15 (Fig. 3) en una base de datos almacenada en cada uno de los dispositivos de almacenamiento en masa secundarios 9,10. Cada una de las filas mostradas corresponde a un registro de extensión 16a-16e. Cada registro de extensión 16 se asocia con un registro exteriorizado. Las entradas en una columna de índice 17 comprenden información que refleja un identificador único para el registro asociado exteriorizado. La tabla de registro de extensión 15 comprende además la primera, segunda y tercera columnas de segmentos de datos 18-21. Así, cada registro de extensión en el ejemplo de los dispositivos de almacenamiento en masa secundarios de ejemplo 9,10 puede comprender tres segmentos de datos. Cada sementó de datos en un registro de extensión 16 para un registro exteriorizado incluye datos correspondientes a al menos una parte asociada de una porción de datos del registro exteriorizado. Por corresponder, se entiende que la parte asociada de la porción de datos puede recuperarse completamente a partir de los datos en el registro exteriorizado. Así, los datos en el sementó de datos pueden ser una versión encriptada, codificada o comprimida de la parte asociada de la porción de datos del registro exteriorizado. Preferiblemente, una cadena de autenticación se almacena con cada sementó de datos. La tabla de registro de extensión también incluye una columna del número de versión 21, en la cual se almacena información reflejando un conteo de versiones para el registro exteriorizado. Lo que se ha dicho antes en relación con las entradas en la columna del número de versión 14 de la tabla de la base de datos primaria 11 (Fig. 2) también se aplica para las entradas en la columna del número de versión 21 ilustrada en la Fig. 3. En una implementación alternativa, cada segmento de datos en una de las primera, segunda y tercera columnas de la sección de datos 18-20 puede comprender, o almacenarse con, información diferente reflejando un conteo de versiones válido para sólo ése segmento de datos.

Cuando un registro se crea por un programa de aplicación estando ejecutado en el primer dispositivo procesador 1 y usando la invención, el primer dispositivo procesador 1 va a través de fases mostradas en la Fig. 4. En una primera fase 22, se inicia un contador de versiones. Por ejemplo, cuando se usan números secuenciales, el contador de versiones se fija en el valor cero, es decir, se incrementa de menos uno a cero. El programa de aplicación hace entonces el registro activo y procede a procesarlo con normalidad. Durante el procesamiento, los datos del registro, los cuales se modifican por el programa de aplicación, se almacenan en el dispositivo de almacenamiento en masa primario 4. En algún punto, el programa de aplicación puede determinar que el registro no se va a seguir procesando, o que existe otra razón para exteriorizar el registro. Por tanto, se inicia la exteriorización del registro, haciendo una llamada a una interfaz. Tal y como se menciona, esta puede ser una interfaz del programa de aplicación proporcionada como parte del sistema operativo del primer dispositivo procesador 1 o por otro programa de aplicación.

Se asume que al menos la CPU 2, la memoria principal 3 y el dispositivo de almacenamiento en masa primario 4 son parte de un entorno seguro, y que los datos del registro se van a proteger. Así, en una segunda etapa 23, se encriptan los datos del registro y se calcula al menos una cadena de autenticación para los datos. En una etapa posterior 24, se escribe un registro primario en la tabla de la base de datos primaria 11 en el dispositivo de almacenamiento en masa primario 4. Esto implica introducir información reflejando un identificador único para el registro que se está exteriorizando en una entrada correspondiente en la columna de índice 13. Además, el conteo de versiones se escribe en una entrada en la columna del número de versiones 14. Así, un objeto de datos de referencia se almacena en el dispositivo de almacenamiento en masa primario 4 para el registro exteriorizado, incluyendo el objeto de datos de referencia un identificador único y una copia de la información que refleja el conteo de versiones.

Entonces, la porción de datos encriptada del registro se transfiere al segundo dispositivo procesador 5, junto con una cadena de autenticación e información reflejando el conteo de versiones, en la etapa 25. El segundo dispositivo procesador 5 almacena el contenido de la sección de datos transferida en la tabla del registro de extensión 15.

Según la invención, un programa de aplicación usando un registro que se ha exteriorizado también puede decidir de manera autónoma interiorizar el registro nuevamente. Una forma de realización del proceso de interiorización se ilustra en la Fig. 5. Así, en algún punto, el programa de aplicación usando, es decir configurado para usar, los datos del registro, determina si el registro debe interiorizarse. El programa de aplicación hace una llamada a una interfaz con el sistema de almacenamiento secundario. El software, por ejemplo una interfaz de programa de aplicación, que es parte de la interfaz con el sistema de almacenamiento secundario asegura que se envía un mensaje al segundo dispositivo procesador 5, solicitando secciones de datos incluyendo datos correspondientes a datos de un registro exteriorizado. El mensaje incluye al menos información reflejando el identificador único para el registro exteriorizado. Esta información se recupera a partir de la entrada asociada en la columna de índice 13 de la tabla de la base de datos primaria 11. La interfaz asegura que al menos una sección de datos incluyendo datos correspondientes a al menos una parte asociada de la porción de datos almacenada externamente, se recupera en la etapa 26. La sección de datos recuperada incluye información reflejando un conteo de versiones. Esta información se obtiene de de la entrada asociada en la columna del número de versión 21 de la tabla del registro de extensión 15. En la fase 27, el primer dispositivo procesador 1 desencripta la parte encriptada de la porción de datos en la sección de datos recuperada, usando una clave de encriptación secreta. Después calcula una cadena de autenticación de verificación de los datos desencriptados. La cadena de autenticación de verificación se compara en la etapa 28 con una cadena de autenticación incluida en la sección de datos recuperados. Si las dos coinciden, un conteo de versiones se deriva de la información incluida en la sección de datos recuperada, y se compara con un conteo de versiones derivado de una introducción en la columna del número de versión 14 de la tabla de base de datos primaria 11. Si las dos coinciden, la porción de datos descifrada se utiliza para ensamblar el registro ahora interiorizado. El registro interiorizado se almacena en el dispositivo de almacenamiento en masa primario 4 para el uso por el programa de aplicación.

Se asumirá que el programa de aplicación que se está ejecutando en el primer dispositivo procesador 1 en realidad modifica los datos del registro (etapa 29). Después de la modificación, de nuevo puede decidir si el registro se debe exteriorizar. En este caso, se actualiza el conteo de versiones, es decir se incrementa, en la etapa 30. Se encripta una porción de datos del registro y se calcula una cadena de autenticación para ésta en la etapa 31. Después, se reescribe el registro primario en la tabla de la base de datos primaria 11, es decir la información reflejando el conteo de versiones incrementado se escribe en la entrada correspondiente en la columna del número de versión 14. Una sección de datos, incluyendo la porción de datos encriptada, la cadena de autenticación y una copia de la información reflejando el conteo de versiones actualizado se transfiere al segundo dispositivo procesador 5, dónde el registro de la extensión correspondiente 16 en la tabla del registro de extensión 15 se actualiza, o se reescribe de nuevo si se ha borrado.

Se observa que una forma de realización preferida de la invención toma cuenta de las características de la CPU 2 y/o la memoria principal 3 y/o el enlace de datos 6. Esto se ilustra en la Fig. 6. Mientras una parte de una porción de datos 34 de un registro se procesa para su inclusión en una sección de datos a transferir o recuperar de una sección de datos recuperada, se mantiene en la memoria principal 3. La capacidad de la CPU 2 o la memoria principal 3 puede ajustar así un enlace al tamaño de la parte, sobre la cual la interiorización y exteriorización ralentizaría de forma inaceptable el primer dispositivo procesador 1. Otro límite para el tamaño de la parte de una porción de datos es el tamaño de la sección de datos resultante, incluyendo la parte encriptada, la cadena de autenticación y el conteo de versiones y la información del índice. Teniendo en cuenta la más limitadora de las limitaciones mencionadas arriba, el primer dispositivo procesador 1 divide la porción de datos 34 de un registro a exteriorizar en varias partes 35-37 en una primera etapa 38. En este caso, están la primera, segunda y tercera partea 35-37. La división en partes 35-37 se puede realizar aplicando del programa de aplicación que procesa el registro, o ejecutando un módulo de una interfaz del programa de aplicación llamada por el programa de aplicación. En una etapa posterior 39, cada una de las partes 35-37 se encripta separadamente usando una clave de encriptación secreta 40, almacenada dentro del entorno seguro del cual el dispositivo de almacenamiento en masa primario 4 y la CPU 2 y la memoria principal 3 también forman parte. Un primer segmento de datos 41 corresponde a una primera parte 35 de la porción de datos 34 del registro que se está exteriorizando, un segundo segmento de datos 42 corresponde a una segunda parte 36 y un tercero segmento de datos 43 corresponde a una tercera parte 37.

En una siguiente etapa 44 una primera cadena de autenticación 45 se calcula para la primera parte 35 de la porción de datos 34, usando el primero segmento de datos 41 como entrada, al igual que una clave de autenticación secreta 46. La clave de autenticación secreta 46 también se almacena dentro del entorno seguro del cual el dispositivo de almacenamiento en masa primario 4 y la CPU 2 y la memoria principal 3 también forman parte. En una siguiente etapa 47, se crea una primera sección de datos 48. La primera sección de datos 48 incluye el primer segmento de datos 41, la primera cadena de autenticación 45, información correspondiente al valor del índice almacenado en la entrada en la columna del índice 13 de la tabla de base de datos primaria 11 para el registro exteriorizado, e información reflejando el hecho de que la primera sección de datos 48 se une con la primera parte 35 en la secuencia de partes 35-37 componiendo la porción de datos 34. Esta primera sección de datos 48 se transfiere después al segundo dispositivo procesador 5 para el almacenamiento.

Al mismo tiempo, una segunda cadena de autenticación 49 se calcula en la etapa 50. La segunda cadena de autenticación 49 se calcula a partir del segundo segmento de datos 42 y la primera cadena de autenticación 45. Esto puede hacerse, por ejemplo, en primer lugar concatenando el segundo segmento de datos 42 con la primera cadena de autenticación 45 y después sometiendo el resultado al mismo algoritmo de autenticación que usa la clave de autenticación 46 como se usó en la etapa 44.

En la etapa 51 se crea una segunda sección de datos 52. La etapa 51 se corresponde con la etapa 50. Así, la segunda sección de datos 52 comprende el segundo segmento de datos 42, la segunda cadena de autenticación 49 e información reflejando un identificador único para el registro exteriorizado, al igual que información reflejando el hecho de que la segunda sección de datos 52 se une con la segunda parte 36 en la secuencia de partes 35-37 formadas a partir de la porción de datos 34.

En la etapa 53, se calcula una tercera cadena de autenticación 54, usando la segunda cadena de autenticación 49 como entrada, al igual que la clave de autenticación 46 y el tercer segmento de datos 43. La etapa 53 se corresponde sustancialmente con la etapa 50.

En la etapa 55 se crea una tercera sección de datos 56 y se transfiere al segundo dispositivo procesador 5. Similar a la primera y la segunda sección de datos 48,52, la tercera sección de datos 56 incluye el tercer segmento de datos 43, la tercera cadena de autenticación 54 e información reflejando un identificador único para el registro exteriorizado, al igual que información reflejando el hecho de que la tercera sección de datos 56 se une con la tercera parte 37 en la secuencia de partes formada a partir de la porción de datos 34.

Nótese que el método de la invención puede aplicarse simultáneamente a porciones de datos de otros registros diferentes al primero al cual pertenece la porción de datos 34. Las secciones de datos 48,52,56 asociadas a las partes 35-37 de la porción de datos 34 de un registro no contiene, sin embargo, segmentos de datos asociados a partes de una porción de datos de otro registro. Esto asegura que la primera, la segunda y la tercera sección de datos 48,52,56 mantienen un tamaño apropiado para el enlace de datos 6. También asegura un procesamiento eficaz mediante el segundo dispositivo procesador 5. En particular, cuando el registro se interioriza de nuevo, se recuperan copias exactas de la primera, segunda y tercera sección de datos 48,52,56. Para prevenir la transferencia de datos innecesaria, es ventajoso separar secciones de datos creadas para un registro de aquellos creados para otro.

La Fig. 7 ilustra un ejemplo específico de un sistema en el cual se procesan registros, lo cual es adecuado para la aplicación de la invención. El sistema ilustrado es un sistema multimedia adaptado para proporcionar acceso a al menos una porción consecutiva de contenido digital y comprendiendo un sub-sistema de acceso condicional para controlar el acceso al contenido digital. Específicamente, la Fig. 7 muestra un aparato de vídeo personal 57 para grabar y manejar datos de contenido descargados de o recibidos en una radiotransmisión desde un distribuidor de contenido de este tipo.

El aparato de vídeo personal comprende un sintonizador 58 para entonar a una frecuencia portadora específica. Comprende además un desmodulador 59 para recuperar una corriente de transporte incluyendo una o más corrientes elementales portando contenido digital. Estas podrían ser por ejemplo corrientes elementales en MPEG-2 o corrientes de unidades de acceso en MPEG-4. Las corrientes elementales se procesan mediante un procesador multimedia 60, el cual tiene acceso a la memoria principal 61 para este propósito. El procesador multimedia 60 se conecta a un bus del sistema 62, por ejemplo un bus 12 áC. El procesador multimedia 60 se conecta posteriormente a un codificador de vídeo 63 y un Conversor de audio Digital-a-Analógico (DAC) 64. Así, el aparato de vídeo personal es capaz de hacer señales analógicas de vídeo y audio disponibles para un dispositivo reproductor, tal como una televisión, a través de salidas apropiadas. Por supuesto, en una forma de realización alternativa, el aparato de vídeo personal también podría comprender un codificador para hacer una salida disponible en forma de una corriente codificada en MPEG-2 (desprotegida) portada, por ejemplo a través de una Ethernet o una red doméstica IEEE 1394 a uno o más dispositivos terminales de una red doméstica.

Un controlador de interfaz 65 también se conecta al bus del sistema 62. El controlador de interfaz 65 retransmite los comandos desde un usuario al procesador multimedia 60 controlando la operación del aparato de vídeo personal 57, y opcionalmente puede proporcionar información retroactiva al usuario. Por ejemplo, el controlador de interfaz podría controlar un puerto infrarojo para aceptar comandos desde una unidad de control remoto (no mostrada) o podría controlar una interfaz del panel frontal del aparato de vídeo personal 57.

El aparato de vídeo personal 57 comprende además un controlador de disco 66, conectado al bus del sistema 62, y a una disquetera óptica 67 y una unidad de disco duro 68. La disquetera óptica 67 y la unidad de disco duro 68 deben considerarse meramente como representativo de unidades de almacenamiento en masa comprendidas en un sistema de almacenamiento de datos secundario para el uso en el método según la invención.

El sub-sistema de acceso condicional comprende un módulo de acceso condicional (CAM) 70, incluyendo un procesador 71 para dirigir las comunicaciones a y desde el módulo de acceso condicional 70. El CAM 73 comprende adicionalmente un co-procesador criptográfico 72, un procesador de señales digitales dedicado a llevar a cabo las operaciones de encriptación y/o desencriptación. Ejemplos de tales CAMs 70 se conocen de aplicaciones de Transmisión de Video Digital (DVB), en las cuales el CAM 70 comunica con un decodificador de recepción integrado, del cual el aparato de vídeo personal 57 es un ejemplo particular, a través de una interfaz común (Cl). En estas aplicaciones conocidas, el módulo de acceso condicional 70 tiene forma de una tarjeta PCMCIA.

El sub-sistema de acceso condicional comprende además una tarjeta inteligente 72, llevando un Circuito Integrado de tarjeta inteligente (IC) 73. La tarjeta inteligente 72 preferiblemente cumple con el estándar ISO 7816-2. La tarjeta inteligente 72 se conecta con el CAM 70 y a través de él, al aparato de vídeo personal 57, a través de un sistema de interconexión física, comprendiendo una almohadilla de contacto (no mostrada) en la tarjeta inteligente y pasa-

dores de contacto (no mostradas) en el CAM 70, y uno o más módulos de software implementando un protocolo de comunicación.

La Fig. 8 muestra que la tarjeta inteligente IC 73 incluye una unidad de procesamiento central (CPU) 74. Además incluye tres tipos de módulo de memoria, es decir, una Memoria de Sólo Lectura de máscara (ROM de máscara) 75, una Memoria de Acceso Aleatorio (RAM) 76 y una Memoria de Sólo Lectura Programable y Borrable Electrónicamente (EEPROM) 77. Por supuesto, la tarjeta inteligente IC 73 también comprende un puerto de entrada/salida (I/O) 78 como parte de la interfaz para el CAM 70. Formas de realización alternativas de la tarjeta inteligente IC 73 podrían comprender una Memoria de Acceso Aleatorio Ferro-eléctrica en lugar de la EEPROM 77.

El ROM de máscara 75 es una memoria no volátil. El sistema operativo de la tarjeta inteligente 72 se almacena en el ROM de máscara 75. Ejemplos de sistemas operativos adecuados son MULTOS, Javacard y Windows Card. Adicionalmente, se pueden almacenar una o más claves secretas en el ROM de máscara 75. La RAM 76 forma el espacio de trabajo de la memoria. RAM 76 es una memoria volátil, y todos los datos se pierden cuando se elimina el suministro de energía a la tarjeta inteligente IC 72. La EEPROM 77 representa memoria de almacenamiento no volátil para almacenar datos de aplicación dinámica.

De los tres tipos de memoria comprendida en la tarjeta inteligente IC 73, la RAM 76 es generalmente la más cara, seguida de la EEPROM 77 y el ROM de máscara 75, en ese orden. En consecuencia es ventajoso mantener la cantidad de memoria limitada, especialmente de los tipos más caros.

Interiorizando y exteriorizando registros comprendidos en los datos de la aplicación dinámica almacenados en una unidad de almacenamiento de datos primaria de la tarjeta inteligente 72, es decir la EEPROM 77, la tarjeta inteligente 72 se las arregla con una EEPROM 77 de capacidad limitada. Dividiendo porciones de datos pertenecientes al registro que se interiorizan y exteriorizan en partes, como parte del método según la invención, la tarjeta inteligente IC 73 puede operar con una RAM 76 de tamaño limitado y un puerto l/O 78 de capacidad limitada.

Un sistema de transmisión en el cual típicamente se usa el sistema multimedia ilustrado en la Fig. 7, comprende un sistema de administración de suscriptores (SMS) donde se guardan los detalles de todos los suscriptores. Información tal como los canales y eventos para los que que el suscriptor está habilitado, su estado de pago, si su tarjeta inteligente 72 está activa o no y otra información se guarda en el SMS. Un evento se define como una porción consecutiva de contenido digital, p. ej. una porción de un servicio de DVB MPEG-2, que está sujeto a un acceso condicional y tiene información de evento asociada. Un evento se codifica con una o varias palabras de control como claves para el algoritmo de codificación. A partir del SMS, se emiten las facturas para el pago de las suscripciones. El SMS controla las tarjetas inteligentes 72 distribuidas a los suscriptores enviándoles comandos a través de un sistema de acceso condicional (CA). El sistema CA transforma estos comandos en el formato correcto para la tarjeta inteligente 72 e inserta los comandos en una corriente de transporte. Otra función del sistema CA es encriptar palabras de control con las cuales se encripta un evento cuando se transmite a los suscriptores. Estas palabras de control encriptadas se transmiten con el contenido que forma el evento como mensajes de control de derecho de acceso (ECMs).

El contenido ofrecido y cada evento que ocurre en la transmisión se programan por un sistema de programación. El contenido se codificada/comprime mediante servidores de contenido. Los datos formateados a partir de los servidores de contenido y el sistema CA se multiplexan en una corriente de transporte que se modula después para la red de transmisión apropiada (es decir, satélite, cable, terrestre, Internet, etc.).

El aparato de vídeo personal 57 usa el sintonizador 58 y el desmodulador 59 para recuperar la corriente de transporte. La corriente de transporte, la cual está encriptada, se rutea al módulo de acceso condicional 70 mediante el procesador multimedia 60. El subsistema de acceso condicional decodifica la corriente de transporte usando una jerarquía de claves. Almacenada en la tarjeta inteligente 72, por ejemplo en el ROM de máscara 75 hay una clave única para la tarjeta inteligente 72, conocida como el ClaveX. En algunos sistemas alternativos puede haber una jerarquía de Claves-X, de las cuales las de nivel más alto se denominan claves de grupo y se asignan a grupos de suscriptores. Para más simplicidad, esta descripción debe asumir un sólo nivel.

El sistema multimedia comprende uno o más módulos de software, de los cuales al menos algunos se instalan en la tarjeta inteligente 72 (otros se pueden instalar en el aparato de vídeo personal 57 o el CAM 70), que implementa un Sistema de Gestión de Eventos (EMS). El sistema de gestión de eventos comprende una aplicación que funciona en la tarjeta inteligente 72, que procesa los procesos conteniendo información usada para controlar el acceso a los eventos. Estos registros incluyen registros de sesión y registros de evento. Mientras los registros de evento y los registros de sesión se están procesando, están activos, y se almacenan en la EEPROM 77. Ambos registros de evento y registros de sesión se pueden exteriorizar transfiriendo al menos una porción de datos del registro a un dispositivo de almacenamiento en un sistema de almacenamiento secundario, por ejemplo a la unidad de disco duro 68 en el aparato de vídeo personal 57.

En una forma de realización ilustrativa, los registros de evento incluyen los siguientes campos: un indicador activo, un indicador cambiado, un número de versión, una identificación del registro, una cuenta pregrabada y una cuenta del número de copias. El indicador activo se establece cada vez que el registro de evento está activo. Un registro de evento está activo al menos cuando el evento se está grabando, copiando o reproduciendo. Cuando un registro de evento está activo, éste se procesa por la CPU 74 de la tarjeta inteligente y los datos del registro se almacenan en la EEPROM

77. Si, en el curso del procesamiento del registro de evento, se hace un cambio en cualquiera de los datos del registro de evento, el indicador cambiado se establece. La virtud de tener un indicador cambiado es que se pueden evitar las exteriorizaciones innecesarias. En la forma de realización preferida, cuando se recibe un comando para exteriorizar el registro del evento, se hace primero un control del indicador cambiado. Si éste no está establecido, la exteriorización no es necesaria, ya que la copia almacenada en el aparato de vídeo personal 57 todavía es precisa. El número de versión se incrementa antes de cada exteriorización del registro del evento. La identificación del registro permite identificar el registro del evento en las llamadas hechas a y mediante la interfaz de la aplicación de programa en la tarjeta inteligente 72. La cuenta pregrabada y la cuenta del número de copias son ambas tipos de información reflejando una cuenta pregrabada, la cual se incrementa cada vez que el registro del evento se hace activo para proporcionar acceso al evento asociado. Esto ocurrirá siempre que se requiera el acceso para el evento, por ejemplo para hacer una copia del evento, para desencriptarlo y decodificarlo, para grabarlo en un disco óptico insertado en la disquetera óptica 67 o en la unidad de disco duro 68, etc.

Los registros de sesión incluyen información de acceso condicional y claves del programa (Claves-P). Las Claves-P son necesarias para desencriptar las palabras de control encriptadas contenidas en los ECMs que se reciben, y pueden grabarse como parte de la corriente de transporte encriptada, mediante el aparato de vídeo personal 57. Las Claves-P y la información de acceso condicional para un evento se obtienen pagando por el evento, a partir de lo cual el sistema CA del transmisior transmite uno o más mensajes de administración del derecho de acceso (EMMs), comprendiendo la información de acceso condicional y las Claves-P, encriptado bajo la Clave-X de la tarjeta inteligente 72. La tarjeta inteligente 72 recupera las Claves-P y la información de acceso condicional de los EMMs y las añade a un registro de sesión. Hay un registro de sesión para cada sesión de grabación, es decir cada periodo temporal consecutivo durante el cual se registran los datos de contenido en la unidad de disco duro 68 o en un disco en la disquetera óptica 67. Cada registro de sesión se enlaza con uno o más registros de evento y se asocia así a los eventos con los cuales están asociados estos registros de evento. El acceso a uno de los eventos está provisto en el curso de una sesión de visualización para cuyo tiempo el registro de sesión está activo, es decir los datos del registro de sesión está presente en la EEPROM 77. El registro del evento también está activo durante el pregrabado del evento.

Para permitir la exteriorización y la posterior interiorización del evento y el registro de sesión, la tarjeta inteligente 72 comprende una interfaz del programa de aplicación, dispuesto para recibir y procesar mensajes de una aplicación implementando las EMS, y así usando los registros de evento y de sesión. Asumiendo que un evento se ha grabado durante una sesión y que las Claves-P necesarias para acceder al evento se han almacenado en un registro de sesión asociado, la aplicación que controla el registro, y que de ese modo usa el registro de evento y de sesión, hace una llamada de exteriorización a la tarjeta inteligente API implementando la exteriorización de registros cuando la grabación ha finalizado y no se requiere ningún pregrabado inmediato. La siguiente descripción se centrará en la exteriorización del registro de evento, bajo la comprensión de que la exteriorización del registro de sesión se realiza de una manera similar.

En una forma de realización, el API divide una porción de datos del registro, la cual puede comprender todos los datos del registro o un sub-conjunto del mismo, en una secuencia de partes consecutivas. Cada parte se dimensiona conforme a la capacidad de procesamiento máxima de la interfaz entre la EEPROM 77 y la unidad de disco duro 68 del aparato de vídeo personal 57. La capacidad de procesamiento máxima se puede determinar por el tamaño de la RAM 76, la unidad de procesamiento central 74, el puerto l/O 78, el procesador 70, la interfaz de PCMCIA entre el CAM 69 y el aparato de vídeo personal 57, o el tamaño del bus del sistema 62, dependiendo de la implementación particular.

Posteriormente, el API recibe un mensaje de exteriorización para cada parte, cada mensaje de exteriorización representa un pedido para transferir una sección de datos incluyendo datos correspondientes a al menos una parte asociada de la porción de datos a transferir. El API genera las secciones de datos usando el método que se describe en relación con la Fig. 6. Es decir, cada parte de la porción de datos del registro de evento se encripta y se calcula un valor de autenticación para la misma. Para cada parte de la porción de datos, se crea una sección de datos separados, comprendiendo el valor de autenticación calculado, la parte encriptada de la porción de datos, y la posición de la parte en la secuencia de partes creadas al dividir la porción de datos en partes consecutivas. Además, la sección comprende información reflejando el número de versión.

El API recibe un mensaje de exteriorización separado para cada sección de datos. Las secciones de datos creadas usando el método ilustrado en la Fig. 6 se devuelven una a una, cada una en respuesta a un mensaje de exteriorización asociado. Estos mensajes de exteriorización comprenden información correspondiente a la identificación del registro de evento y la información identificando la sección de datos mediante la posición de la parte asociada de la porción de datos en la secuencia de partes. Opcionalmente, el API puede devolver información representando cuántas partes hay en la secuencia en respuesta a la primera llamada recibida.

Después de haberse transferido la sección de datos, la aplicación envía un pedido de confirmación. Si se confirma una exteriorización correcta, se restablece el indicador cambiado en la copia de los datos del registro guardada en la EEPROM 77. Sólo entonces el registro puede hacerse inactivo y la porción de datos del registro que fue transferida a la memoria externa se puede borrar de la EEPROM 77. No obstante, se guarda un objeto de datos de referencia en la EEPROM 77 para cada registro exteriorizado. El objeto de datos de referencia incluye la identificación del registro, y el número de versión.

Cuando el registro de evento se interioriza de nuevo, por ejemplo para permitir el pregrabado del evento asociado, la tarjeta inteligente API recibe una llamada de una aplicación usando datos del registro del evento. El API entonces recupera las secciones de datos almacenadas en la unidad de disco duro 68. Nuevamente, las secciones de datos se recuperan y procesan separadamente. Donde cada sección de datos incluye datos correspondientes a una parte de una porción de datos del registro con una posición bien definida en una secuencia, las secciones de datos se recuperan en orden. Así, la sección de datos incluyendo datos correspondientes a la primera parte en la secuencia se recupera primero. Esto es necesario para poder calcular un valor de autenticación de referencia para cada sección sin tener que guardar primero todas las secciones de datos. Sólo el valor de autenticación de referencia para la primera sección se puede calcular sin usar los valores de autenticación de referencia calculados para una o más de las otras secciones de datos. Nótese que el uso de valores de autenticación de referencia calculados evita la necesidad de almacenar valores de autenticación de referencia. Sólo se debe almacenar una clave de autenticación. La clave de autenticación se puede almacenar en el ROM de máscara 75, que es menos caro que la EEPROM 77. De forma alternativa, ésta se puede almacenar en la EEPROM 77 para permitir un cambio de clave de autenticación durante la vida de la tarjeta inteligente 72.

La sección de datos se desencripta usando la clave de encriptación almacenada en la tarjeta inteligente 72 (se asume que se usa un algoritmo simétrico). Después, el número de versión incluido con la sección de datos se compara con el valor de autenticación de referencia calculado y el número de versión del registro de evento se compara con el número de versión almacenado en el objeto de datos de referencia almacenado en la EEPROM 77. Si ambos son correctos, el proceso se repite para cada una de las secciones de datos posteriores, y la porción de datos del registro de evento se reensambla en la EEPROM 77. Después de esto, se puede activar el registro de evento y los datos recuperados de éste para permitir que el sub-sistema de acceso condicional controle la reproducción, la copia u otro uso de un evento almacenado en la unidad de disco duro 68.

Debido a que los datos del registro de evento se almacenan externamente en forma encriptada, es difícil para los piratas informáticos, por ejemplo, reducir la cuenta de reproducciones para permitir más visualizaciones de las que se permiten según la información sobre el acceso condicional en un registro de sesión. Aunque el pirata informático deduzca la clave de encriptación, después sería necesaria la clave de autenticación para calcular un valor de autenticación nuevo para una sección de datos conteniendo información correspondiente a la cuenta de reproducciones reducida. Puesto que se usa el encadenamiento, los valores de autenticación para todas las demás secciones de datos asociadas al registro de evento también se necesitarían. No es posible simplemente hacer una copia de una sección de datos anterior, porque su número de versión no coincide con el número de versión almacenado en el objeto de datos de referencia en la EEPROM 77 de la tarjeta inteligente 72, de modo que tales secciones de datos anteriores no originarán una interiorización exitosa del registro de evento.

La inclusión de un número de versión en el objeto de datos de referencia que permanece en la EEPROM 77 de la tarjeta inteligente 72 y en las secciones de datos transferidas a la unidad de disco duro 68 habilita un proceso para la sustitución de una primera tarjeta inteligente por una segunda tarjeta inteligente a implementar. Una segunda tarjeta inteligente dispone de datos correspondientes a los datos en el objeto de datos de referencia en la primera tarjeta inteligente, preferiblemente de una tercera parte fiable, tal como el sistema CA que transmite datos al aparato de vídeo personal 57. La segunda tarjeta inteligente puede entonces interiorizar el registro usando los datos proporcionados. Cuando posteriormente exterioriza el registro nuevamente, el número de versión se incrementa. Así, la primera tarjeta inteligente ya no interiorizará el registro, puesto que está almacenando un objeto de datos de referencia con el número de versión precedente para el registro. Por supuesto, la segunda tarjeta inteligente debe proveerse de la clave de encriptación y de autenticación, al igual que del objeto de datos de referencia.

La invención no está limitada a las formas de realización anteriormente descritas, pero pueden variarse dentro del alcance de las reivindicaciones adjuntas. Por ejemplo, el sistema comprendiendo el aparato de vídeo personal 57 y el módulo de acceso condicional 69 con la tarjeta inteligente 72 insertada es representativa de sistemas multimedia similares que son adecuados de forma similar para la aplicación de la invención. Esto incluye sistemas incluyendo una caja de conversión en vez del aparato de vídeo personal, un ordenador personal con hardware periférico asociado para recibir contenido digital protegido por un método de acceso condicional, o un aparato de vídeo personal dispuesto para recibir una señal analógica.

**Documentos citados en la descripción**

*Esta lista de documentos citados por el solicitante ha sido recopilada exclusvamente para la información del lector y no forma parte del documento de patente europea. La misma ha sido confeccionada con la mayor diligencia; la OEP sin embargo no asume responsabilidad alguna por eventuales errores u omisiones.*

**Documentos de patente citados en la descripción**


- US 5757919 A [0002]
- FR 2803471 A [0004]
- EP 0856818 A2 [0006]
- WO 0026866 A [0008]

## REIVINDICACIONES

1. Método de almacenamiento de datos externo en un sistema incluyendoun dispositivo procesador primario (1,72), teniendo un procesador (2,74) y una unidad de almacenamiento de datos primaria (4,77), adaptado para ejecutar programas de aplicación para procesar registros activos en el procesador (2,74) y configurado para almacenar datos pertenecientes a registros activos en la unidad de almacenamiento de datos primaria (4, 77); y un sistema de almacenamiento de datos secundario (5,57,69), accesible para el dispositivo procesador primario (1,72),incluyendo el método datos de carga pertenecientes a un registro activo en la unidad de almacenamiento de datos primaria (4,77) y exteriorizar el registro transmitiendo al menos una porción (34) de datos, pertenecientes al registro, al sistema de almacenamiento de datos secundario (5,57,69) para el almacenamiento,

**caracterizado** por el hecho de que la etapa de exteriorización de un registro incluye la realización de una llamada, mediante uno de los programas de aplicación que ha estado usando datos pertenecientes al registro, a una interfaz (6-8,60,61,62,66,70,78) dispuesta para transferir la porción (34) de datos al sistema de almacenamiento de datos secundario (5,57,69).

2. Método según la reivindicación 1, incluyendo transferir una sección de datos (48,52,56) incluyendo datos (41-43) correspondientes a al menos una parte asociada (35-37) de sólo una porción (34) de datos a un registro.

3. Método según la reivindicación 1 ó 2, donde la porción (34) de datos se divide en una pluralidad de partes (35-37) y donde una pluralidad de secciones de datos (48,52,56), cada una incluyendo datos (41-43) correspondientes a una de las partes asociadas de la pluralidad de partes (35-37), se transfiere al sistema de almacenamiento de datos secundario (5,57,69) para el almacenamiento.

4. Método según la reivindicación 2 ó 3, donde los datos (41-43) correspondientes a una parte asociada (35-37) se generan encriptando al menos parcialmente la parte asociada (35-37) de la porción de datos (34).

5. Método según cualquiera de las reivindicaciones 2-4, incluyendo calcular un valor de autenticación (45,49,54) para cada parte (35 37) de la porción (34) de datos e incluyendo datos reflejando el valor de autenticación (45,49,54) en la sección de datos (48,52,56) que incluye datos (41-43) correspondientes a esa parte (35-37).

6. Método según la reivindicación 5, incluyendo calcular el valor de autenticación para al menos una parte (36-37) de la porción (34) de datos usando información derivada de otra parte (35,36) como entrada.

7. Método según cualquiera de las reivindicaciones 2-6, incluyendo almacenar un objeto de datos de referencia (11) en una unidad de almacenamiento de datos (4) del dispositivo primario (1) para cada registro exteriorizado, incluyendo un único identificador, donde los datos reflejando el único identificador se incluye en cada sección de datos (48,52,56) que incluye datos (41-43) correspondientes a una parte (35-37) de la porción (34) de datos del registro.

8. Método según cualquiera de las reivindicaciones precedentes, incluyendo almacenar información reflejando un conteo de versiones para el registro exteriorizado e incrementar el conteo de versiones antes de exteriorizar el registro.

9. Método para interiorizar un registro en un sistema incluyendo un dispositivo procesador primario (1,72), teniendo un procesador (2,74) y una unidad de almacenamiento de datos primaria (4,77), adaptado para procesar registros activos en el procesador (2,74) y configurado para almacenar datos pertenecientes a registros activos en la unidad de almacenamiento de datos primaria (4, 77); y un sistema de almacenamiento de datos secundario (5:57,69), accesible para el dispositivo procesador primario (1,72), y dispuesto para almacenar una porción (34) de datos transferidos mediante un método según cualquiera de las reivindicaciones 1-8, incluyendo el método datos de carga pertenecienes al registro en la unidad de almacenamiento de datos primaria (4:77), donde el sistema incluye una interfaz (6-8,60,61,62,66,70,78) para recuperar la porción (34) de datos pertenecientes al registro desde el sistema de almacenamiento de datos secundario (5,57,69), comprendiendo el método además las etapas de un programa de aplicación configurado para usar datos pertenecienes al registro que determina que el registro se debe interiorizar y hacer al menos una llamada a la interfaz (6-8,60,61,62,66,70,78).

10. Método según la reivindicación 9, incluyendo recibir al menos una sección de datos (48,52,56) incluyendo datos (41-43) correspondientes a al menos una parte asociada (35-37) de una porción (34) de datos desde el sistema de almacenamiento secundario (5: 57,69).

11. Método según la reivindicación 10, incluyendo recuperar un identificador único para el registro de un objeto de referencia (11) almacenado en una unidad de almacenamiento de datos (4) del dispositivo procesador primario (1), donde las secciones de datos (48,52,56) se almacenan en el sistema de almacenamiento de datos secundario (5,57,69) con información reflejando el identificador único y se reciben en respuesta a un mensaje de interiorización incluyendo el reflejo de la información del identificador único.

12. Método según cualquiera de las reivindicaciones 9-11, donde la porción (34) de datos comprende una pluralidad de partes (35-37), incluyendo, recibir varias secciones de datos (48,52,56), cada una incluyendo datos (41-43) correspondientes a una de las partes asociadas de la pluralidad de partes (35-37).

13. Método según las reivindicaciones 11 y 12 incluyendo recuperar información reflejando el número de partes (35-37) del objeto de referencia (11) y recibir cada sección de datos (48,52,56) en respuesta a uno de un número correspondiente de mensajes de interiorización.

14. Método según cualquiera de las reivindicaciones 10-13, incluyendo recibir al menos una sección de datos (48,52,56) incluyendo un valor de autenticación (45,49,54), recuperar una porción secreta de información (46) almacenada en el dispositivo procesador primario (1), calcular un valor de autenticación de verificación para cada sección de datos (48,52,56) de al menos parte de los datos (41, 43) correspondientes a al menos una parte asociada (35-37) de la porción (34) de datos, usar la porción secreta de información (46), y comparar el valor de autenticación de verificación y el valor de autenticación (45,49,54) para cada sección de datos (48,52,56).

15. Método según la reivindicación 14, incluyendo recibir una secuencia de secciones de datos (48,52,56), cada una incluyendo un valor de autenticación (45,49,54), donde el valor de autenticación de verificación para al menos una sección de datos (48,52,56) se calcula usando información (45,49) derivada de otra sección de datos (48,52,56) como entrada.

16. Método según cualquiera de las reivindicaciones 10-15, incluyendo recuperar una clave secreta (40) almacenada en el dispositivo procesador primario (1) y desencriptar al menos parte (41-43) de una sección de datos recibidos (48,52,56).

17. Método según cualquiera de las reivindicaciones 10-16, incluyendo recibir una sección de datos (48,52,56) incluyendo información reflejando un conteo de versiones para el registro exteriorizado y comparar el conteo de versiones con un conteo de versiones de referencia.

18. Dispositivo procesador primario, con un procesador (2,74) y una unidad de almacenamiento de datos primaria (4,77), adaptado para procesar registros activos en el procesador (2,74), configurado para almacenar datos pertenecientes a un registro activo en la unidad de almacenamiento de datos primaria (4,77), y adaptado para ejecutar un método según cualquiera de las reivindicaciones 1-17.

19. Medios de programa de ordenador los cuales, al ejecutarse por un dispositivo procesador primario (1,72) teniendo un procesador (2,74) y una unidad de almacenamiento de datos primaria (4,77), permiten al dispositivo procesador primario (1,72) ejecutar un método según cualquiera de las reivindicaciones 1-17.

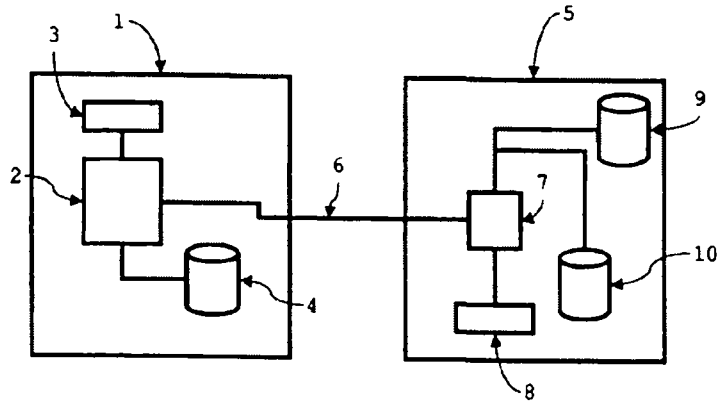


Fig. 1

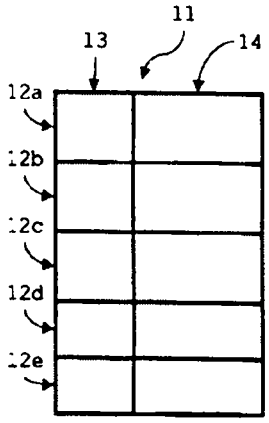


Fig. 2

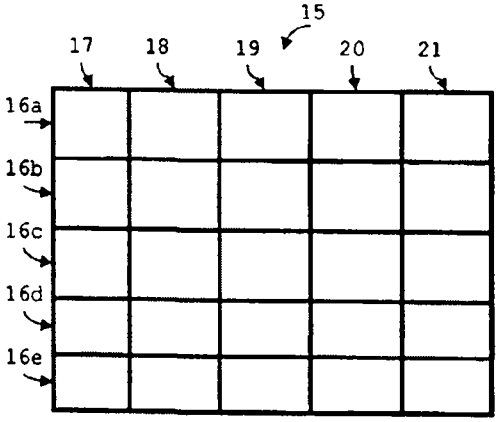


Fig. 3

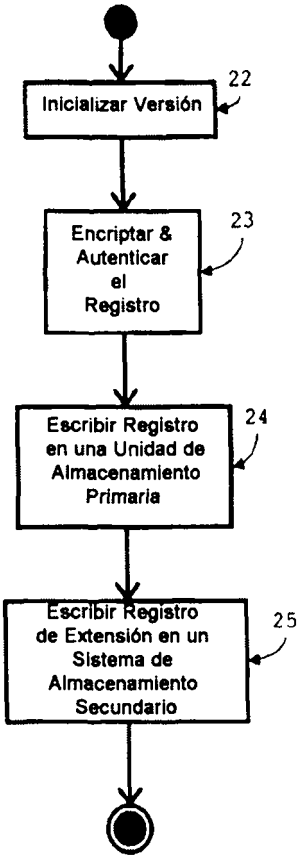
Inicializar Versión
22
Encriptar & Autenticar el Registro
23
Escribir Registro en una Unidad de Almacenamiento Primaria
24
Escribir Registro de Extensión en un Sistema de Almacenamiento Secundario
25

Fig. 4

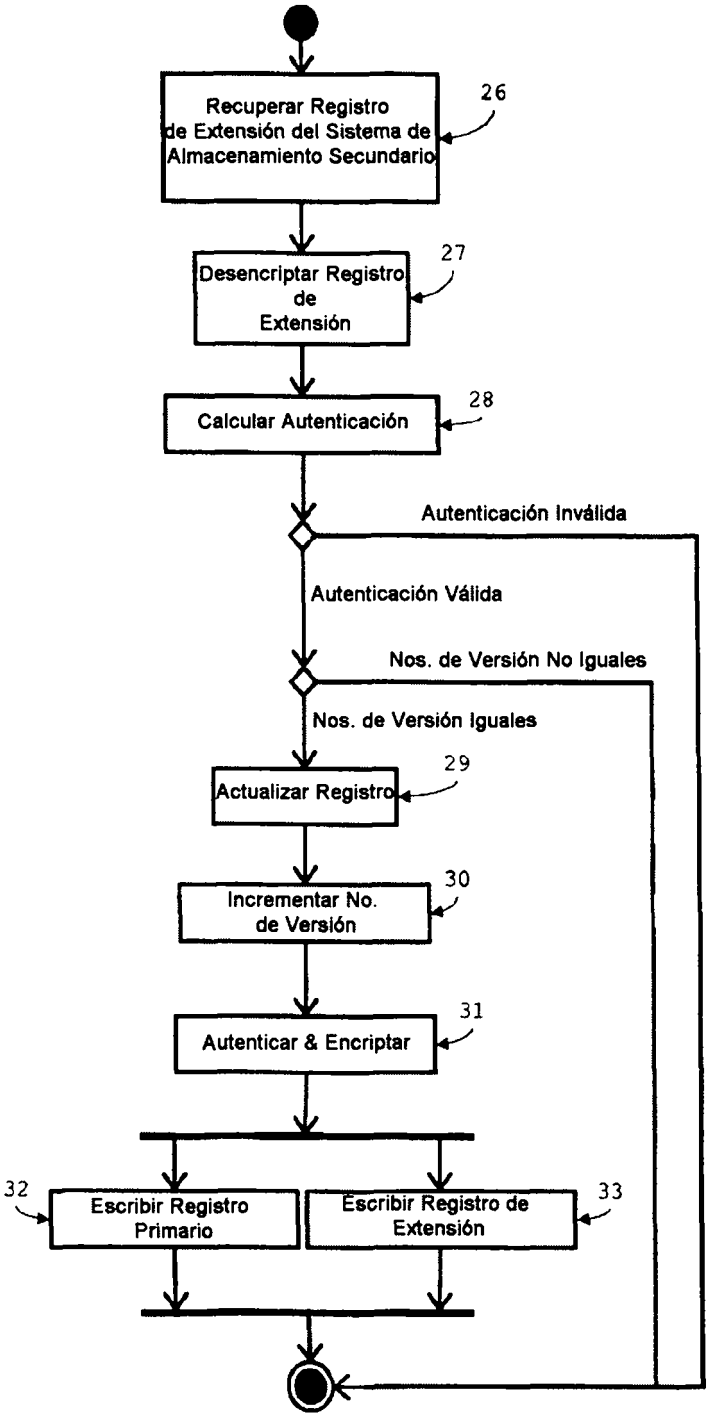
Recuperar Registro de Extensión del Sistema de Almacenamiento Secundario
26
Desencriptar Registro de Extensión
27
Calcular Autenticación
28
Autenticación Inválida
Autenticación Válida
Nos. de Versión No Iguales
Nos. de Versión Iguales
Actualizar Registro
29
Incrementar No. de Versión
30
Autenticar & Encriptar
31
Escribir Registro Primario
32
Escribir Registro de Extensión
33

Fig. 5

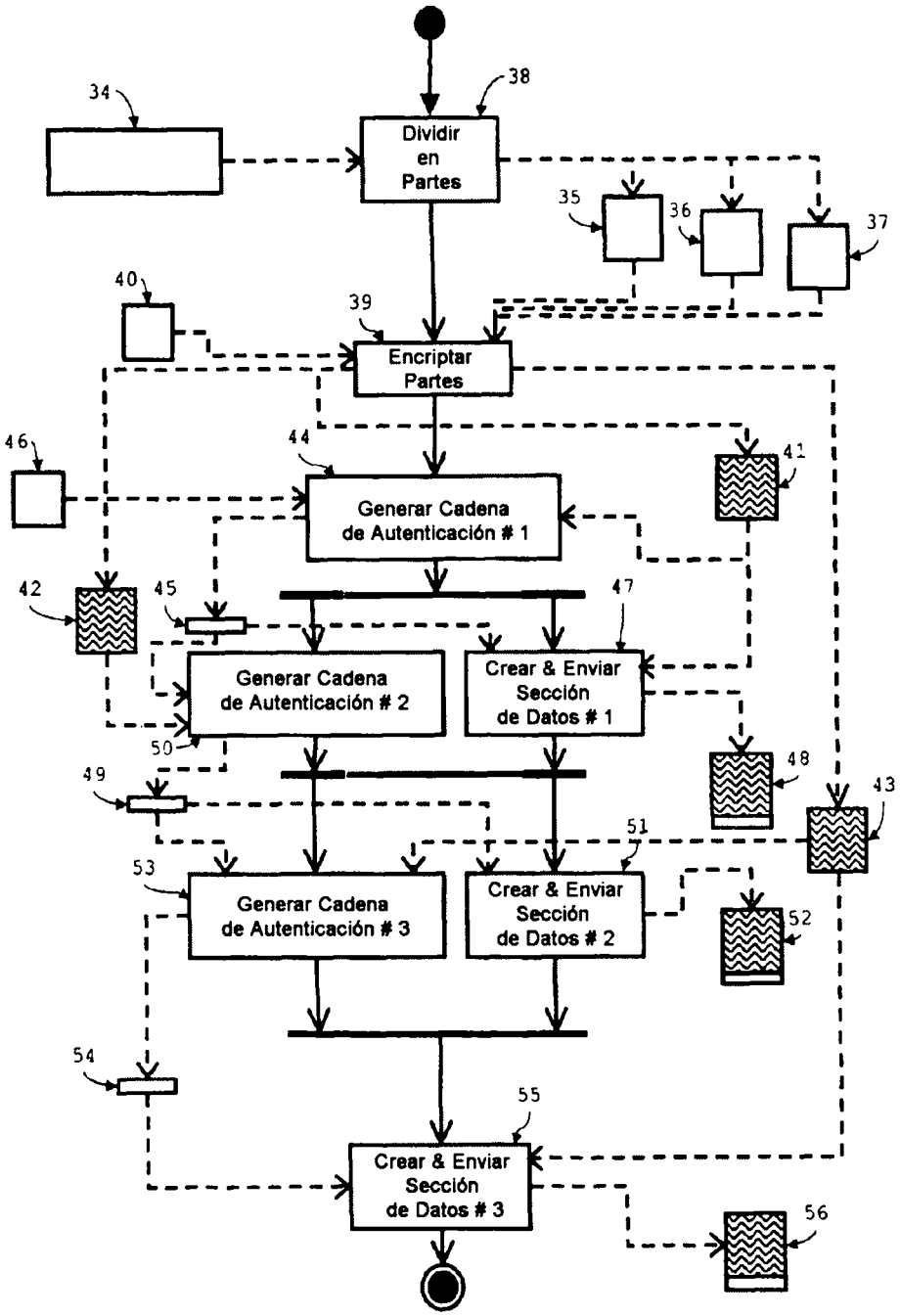
34
38
Dividir en Partes
35
36
37
40
39
Encriptar Partes
46
44
41
Generar Cadena de Autenticación # 1
42
45
47
Generar Cadena de Autenticación # 2
Crear & Enviar Sección de Datos # 1
50
48
49
43
51
53
Generar Cadena de Autenticación # 3
Crear & Enviar Sección de Datos # 2
52
54
55
Crear & Enviar Sección de Datos # 3
56

Fig. 6

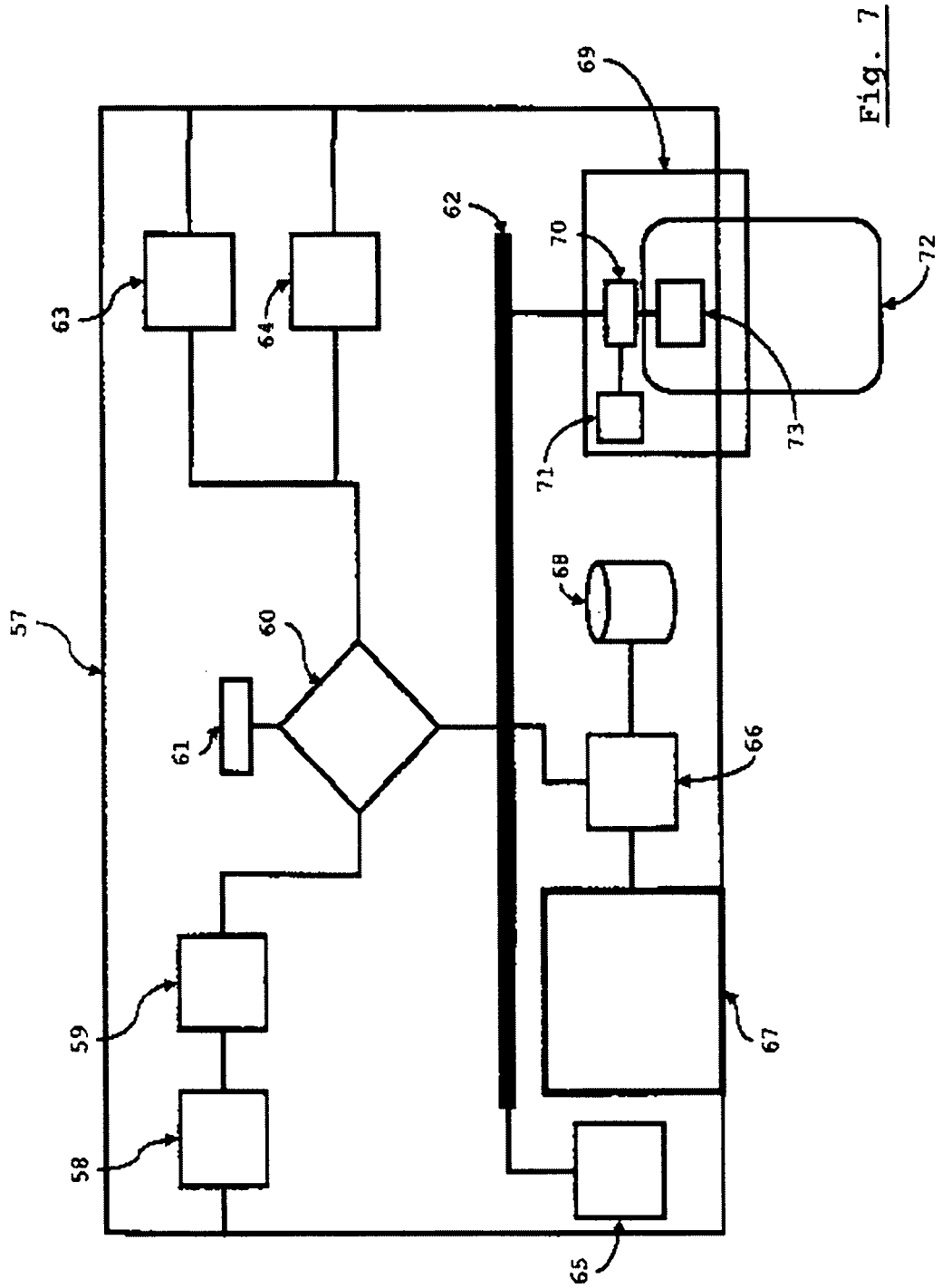


Fig. 7

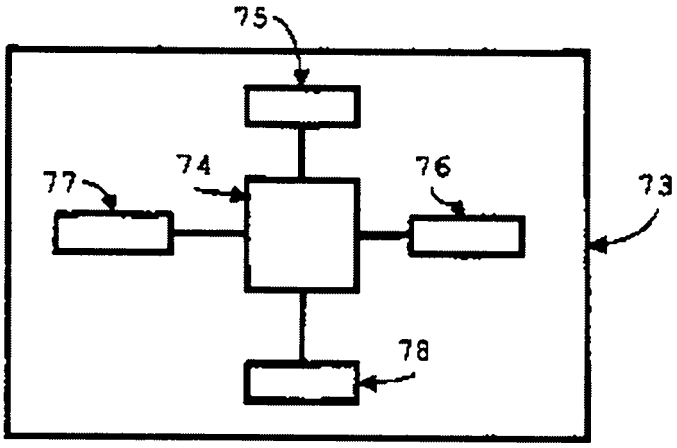


Fig. 8