(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 346 299**

(51) Int. Cl.:
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **02755352 .8**
(96) Fecha de presentación : **10.09.2002**
(97) Número de publicación de la solicitud: **1430639**
(97) Fecha de publicación de la solicitud: **23.06.2004**

(54) Título: **Dispositivo y método de sellado de tiempo.**

(30) Prioridad: **28.09.2001 GB 0123453**

(45) Fecha de publicación de la mención BOPI:
14.10.2010

(45) Fecha de la publicación del folleto de la patente:
14.10.2010

(73) Titular/es: **nCipher Corporation Limited**
Jupiter House, Station Road,
Cambridge CB1 2JD, GB

(72) Inventor/es: **Harvey, Ian Nigel**

(74) Agente: **Elzaburu Márquez, Alberto**

ES 2 346 299 T3

DESCRIPCIÓN

Dispositivo y método de sellado de tiempo.

La invención se refiere a un dispositivo y a un procedimiento para proporcionar sellos de tiempo digitales en documentos u otros datos digitales. Dichos dispositivos pueden ser usados para proporcionar lo que a veces se denomina "Servicios de Notaría Digital".

Los dispositivos que pueden emitir sellos de tiempo digitales en documentos u otros datos digitales, por medio de una firma digital, son útiles en muchas aplicaciones. Típicamente, dichos dispositivos incluyen una fuente de tiempo interna con garantía de exactitud y que no puede ser corrompida por medios externos. La salida de la fuente de tiempo es combinada de alguna manera con el documento u otros datos digitales a los que se debe aplicar un sello de tiempo y, a continuación, la combinación es firmada criptográficamente. Los dispositivos de este tipo conocidos se describen en las patentes US US-A-5.001.752 y US-A-5.136.647.

Una vista generalizada de un dispositivo de sellado de tiempo conocido se muestra en la Figura 1. En el funcionamiento normal, el dispositivo 20 acepta una solicitud de sello de tiempo de un cliente. Al recibir la solicitud, obtiene un valor de tiempo desde una fuente de tiempo o reloj 40, y lo combina con los datos en la solicitud por medio de una firma digital, producida por un generador 50 de firma. El generador de firma hace uso de una clave de firma, que a su vez es mantenida secreta dentro del dispositivo 20 en un almacén 80 de claves.

La salida 55 del dispositivo comprende, de esta manera, una copia con sello de tiempo y firmada digitalmente de la solicitud 22 de sello de tiempo original.

El ajuste del reloj 40 es responsabilidad de una Autoridad de Sellado de Tiempo 10 externa. Cuando la Autoridad de Sellado de Tiempo desea reajustar el reloj, ésta transmite una solicitud 15 de reajuste de reloj que es recibida por un control 30 de acceso a reloj. El control de acceso a reloj comprueba las credenciales presentadas por la Autoridad de Sellado de Tiempo y, si las credenciales son aceptables, permite que el reloj 40 sea reajustado.

La gestión de la clave es responsabilidad de una Autoridad 60 de Claves externa. Un control 70 de acceso a claves recibe señales 65 de gestión de claves desde la Autoridad de Claves y, si se le permite el acceso, actualiza el almacén 80 de claves, de manera correspondiente.

Uno de los problemas con este tipo de dispositivo es que la Autoridad de Claves debe confiar implícitamente en la Autoridad de Sellado de Tiempo para ajustar el tiempo de manera correcta. Frecuentemente, la Autoridad de Claves y la Autoridad de Sellado de Tiempo son organizaciones diferentes: por ejemplo, la Autoridad de Claves puede realizar un servicio que genera unos ingresos usando máquinas que son propiedad de y cuyo mantenimiento es realizado por la Autoridad de Sellado de Tiempo. Entonces, ésta última tiene que asegurar a la primera que sus procedimientos de mantenimiento son completamente fiables.

También es bastante común que la Autoridad de Sellado de Tiempo subcontrate a una tercera parte, tal como un ASP (Proveedor de Servicios de Aplicaciones), la operación de los ordenadores sobre los que realmente funciona el servicio. Para reajustar su propio reloj, la Autoridad de Sellado de Tiempo entra, de manera remota, al ordenador que está siendo utilizado en su nombre dentro del ASP.

Sin embargo, un ASP individual puede desear proporcionar instalaciones para más de una Autoridad de Sellado de Tiempo. Esto es caro, ya que requiere que el ASP proporcione ordenadores seguros individuales para cada Autoridad de Sellado de Tiempo a la que desee servir. El hardware requerido por cada Autoridad de Sellado de Tiempo es esencialmente idéntico, pero debe ser duplicado por razones de seguridad.

Un problema similar surge cuando el ASP desea actuar para un número de Autoridades de Claves diferentes, cada una de las cuales requiere actuar como su propia Autoridad de Sellado de Tiempo (en otras palabras, necesita tener control sobre el tiempo usado en los sellos de tiempo que son emitidos en su nombre). Una vez más, la única solución realista es la duplicación del hardware. El documento US 6.009.177 describe un dispositivo de sellado de tiempo estándar que proporciona sellos de tiempo basados solo en una única Autoridad de Sellado de Tiempo.

Es un objeto de la presente invención mitigar al menos estos problemas de la técnica anterior.

Es un objeto adicional de la invención proporcionar un procedimiento y un dispositivo de sellado de tiempo que pueden ser usados por múltiples autoridades de sellado de tiempo, autoridades de claves y usuarios, a un pequeño costo adicional.

Según un primer aspecto de la presente invención, se proporciona un dispositivo de sellado de tiempo para el sellado de tiempo digital de los datos de entrada, que comprende:

un temporizador (130) que tiene una salida de tiempo;

medios (150) de firma para generar una salida (94) con sello de tiempo

caracterizado por

medios (120) de memoria para almacenar una pluralidad de conjuntos de información (124) de calibración de temporizador, definiendo cada uno características de un reloj virtual respectivo;

medios (140) de compensación para ajustar la salida del temporizador según un reloj virtual seleccionado por el usuario, para generar una salida del reloj virtual seleccionado; y

siendo capaces los medios de firma de generar la salida con sello de tiempo dependiendo de la salida del reloj virtual seleccionado y los datos de entrada.

Según un segundo aspecto, se proporciona un procedimiento de sellado de tiempo digital de datos de entrada, que comprende:

seleccionar un conjunto de información (124) de calibración de temporizador de entre una pluralidad de dichos conjuntos, definiendo cada conjunto las características de un reloj virtual respectivo;

ajustar un salida de temporizador según el conjunto seleccionado para generar una salida del reloj virtual seleccionado; y

firmar los datos representativos tanto de la salida del reloj virtual seleccionado como de los datos de entrada para generar una salida (94) con sello de tiempo.

Con dicho enfoque, se pueden proporcionar diferentes fuentes de tiempo a partir del mismo temporizador, simplemente cambiando los datos de calibración. El temporizador es una pieza de circuitería cara, mientras que los múltiples conjuntos de datos de calibración pueden ser almacenados en un dispositivo de memoria muy barato. Por lo tanto, se puede proporcionar múltiples fuentes de tiempo controlables de manera independiente a un pequeño costo extra.

Preferentemente, los medios de compensación ajustan la salida del temporizador según un algoritmo de compensación. Esto podría ser definido por el usuario (para cada uno de los relojes virtuales), pero más típicamente, ajustará simplemente el desfase y la deriva de la salida del temporizador en comparación con un reloj de referencia con mantenimiento externo, mantenido, por ejemplo, por una Autoridad de Sellado de Tiempo. De esta manera, en una realización simple, la información de calibración del temporizador para cada uno de los relojes virtuales puede consistir simplemente en dos números: el desfase y la tasa de deriva.

Los medios de firma generan la salida con sello de tiempo dependiendo tanto de la salida del reloj virtual seleccionado como de los datos de entrada. Esto podría ser realizado convenientemente simplemente concatenando la salida del reloj virtual seleccionado y los datos de entrada, y firmando la cadena concatenada resultante. Como alternativa, podrían idearse fácilmente otros enfoques para combinar los datos previamente a la firma.

Preferentemente, cada clave de firma puede comprender la parte privada de un par de claves pública/privada dentro de un sistema de criptografía de clave pública, tal como, por ejemplo, RSA y DSA.

Pueden proporcionarse medios de comprobación/control para comprobar las credenciales de cualquier usuario que desee aplicar un sello de tiempo a unos datos usando un reloj virtual particular. De la misma manera, pueden proporcionarse medios de comprobación/control de acceso que permitan a una Autoridad de Sellado de Tiempo cambiar la información de calibración para un reloj virtual particular, y para que una Autoridad de Claves realice las tareas de gestión de claves. Por supuesto, se entenderá que (cuando se proporcionen) los medios de control de acceso a sello de tiempo, los medios de control de acceso a claves y los medios de control de acceso a reloj virtual no son necesariamente entidades separadas físicamente: si es conveniente, pueden estar realizados dentro del mismo hardware y/o dentro de las mismas rutinas de software.

La invención puede ser llevada a la práctica en una serie de maneras y ahora se describirá una realización específica, a modo de ejemplo, con referencia a los dibujos adjuntos, en los que:

La Figura 1 es una vista esquemática generalizada de un dispositivo de sellado de tiempo de la técnica anterior;

La Figura 2 es un dispositivo de sellado de tiempo según una realización de la presente invención; y

La Figura 3 ilustra la manera en la que el dispositivo de sellado de tiempo de la Figura 2 puede ser usado para el sellado de tiempo de un documento realizado.

La invención parte del reconocimiento de que se puede construir un reloj controlable tomando un temporizador de funcionamiento libre y observando si el mismo es rápido o lento en comparación con una fuente de tiempo de referencia. Determinando el desfase y la deriva en comparación con la fuente de tiempo de referencia, puede construirse un conjunto de datos de calibración que puede aplicarse a la salida del temporizador para convertir la salida del temporizador al tiempo "correcto" (es decir, el tiempo tal como se define por la fuente de tiempo de referencia).

Aunque que el concepto de la salida de reloj compensada es, en sí mismo, conocido, el presente solicitante ha llevado el concepto un paso más allá permitiendo la posibilidad de producir diferentes fuentes de tiempo controlables a partir del mismo temporizador de funcionamiento libre, simplemente cambiando los datos de calibración. Esto proporciona una manera de crear múltiples relojes virtuales controlables, todos los cuales usan un temporizador físico común.

La Figura 2 ilustra el dispositivo de sellado de tiempo preferente de la presente invención. Este proporciona múltiples relojes virtuales, usando el mismo temporizador físico, cada uno de los cuales tiene su propio control de acceso, información de calibración y clave de firma digital.

El dispositivo de sellado de tiempo mostrado en la Figura 2 toma preferentemente la forma de un módulo de hardware discreto que tiene un límite de seguridad ilustrado por la línea 90 de puntos. La información almacenada dentro de este límite puede ser extraída y/o modificada solo por los usuarios que presenten credenciales adecuadas. De esta manera, para el usuario, el dispositivo parece ser efectivamente una caja negra que tiene una única entrada 92 y una única salida 94. Como alternativa, para aplicaciones menos exigentes, el dispositivo no necesita estar en un módulo de seguridad separado, sino que podría estar integrado en un sistema de ordenador de propósito general. Algunos o todos los elementos mostrados pueden ser implementados en hardware o, como alternativa, en software.

Tal como se ha indicado anteriormente, el dispositivo incluye una pluralidad de relojes virtuales, estando definidas las características de cada reloj mediante la información almacenada en una memoria 120, concretamente, información 122 de control de acceso, información 124 de calibración e información 126 de claves. Preferentemente, la información de claves comprende un par de claves pública/privada. Todos los relojes virtuales hacen uso de un temporizador 130 común, que puede ser un temporizador de funcionamiento libre o, como alternativa, puede recibir, a su vez, su tiempo desde una fuente 134 externa confiable vía una antena 132 de radio o algún otro medio de comunicación (no mostrado).

Un usuario que desea aplicar un sello de tiempo a un documento o a otros datos, presenta los datos junto con las credenciales de acceso apropiadas en la entrada 92 del dispositivo. Esta información es pasada primero a una sección 100 de identificación que usa la información de identificador dentro de las credenciales para buscar dentro de la memoria 120 la información relacionada con el reloj virtual apropiado que debe usarse. La información 122 de control de acceso para este reloj es pasada a una sección 110 de comprobación de acceso, que comprueba si las credenciales suministradas en la solicitud son correctas o no.

Suponiendo que la comprobación de acceso es positiva, a continuación se lee un valor de tiempo desde el temporizador 130 y es corregido, a continuación, por una sección 140 de compensación usando la información 124 de calibración apropiada para ese reloj

virtual particular. A continuación el tiempo calibrado es pasado a una sección 150 de firma, donde es combinado con los datos originales suministrados en la entrada 92, y es firmado con la clave 126 apropiada correspondiente.

Los datos firmados y con sello de tiempo son pasados, a continuación a la salida 94.

Las solicitudes para calibrar un reloj virtual particular (por ejemplo, en nombre de una Autoridad de Sellado de Tiempo particular) son suministradas también al dispositivo en la entrada 92, junto con las credenciales apropiadas que autorizan al dispositivo a permitir la recalibración. Por supuesto, se entenderá que estas credenciales serán típicamente diferentes de las requeridas para simples solicitudes de sellado de tiempo. Suponiendo que las credenciales son aceptadas por la sección 110 de comprobación de acceso, la información 124 de calibración para ese reloj virtual particular puede ser actualizada. Típicamente, la Autoridad de Sellado de Tiempo puede simplemente suministrar un tiempo de "referencia" en su solicitud, y el mismo es comparado simplemente con un valor de tiempo leído del temporizador 130 para computar un nuevo conjunto de datos de calibración.

El dispositivo responde además a solicitudes realizadas en la entrada 92, con credenciales apropiadas, para realizar operaciones de gestión de claves, tales como fijar la clave, generar una nueva clave, solicitar la mitad pública de la clave de la firma, etcétera. Estas funciones pueden ser requeridas, típicamente, por una Autoridad de Claves externa.

La información 122 de control de acceso, para cualquier reloj virtual determinado, puede definir cómo y hasta qué punto pueden permitirse las solicitudes para cambiar la información 124 de calibración y/o la información 126 de claves.

La modificación de la propia información 122 de control de acceso puede permitirse con la presentación de diferentes credenciales de acceso de alto nivel en la entrada 92.

La Figura 3 ilustra la manera en la que el dispositivo de sellado de tiempo de la Figura 2 puede ser usado en la práctica para el sellado de tiempo de un contrato firmado por dos partes A y B.

Un contrato 200 es enviado separadamente a las dos partes contratantes A 202 y B 204, para su firma. Los contratos firmados individualmente, junto con el contrato original son suministrados a una función 206 hash que concatena las entradas y crea un "mensaje de recopilación" 208. Este es esencialmente representativo único de ambos el contrato original y el hecho de que las dos partes A y B han firmado.

El mensaje de recopilación 208 necesita ahora ser presentado al dispositivo de sellado de tiempo, y en este punto el solicitante 210 del sello de tiempo genera un identificador de mensaje (cabecera) 212 que contiene información relevante, tal como una explicación de qué era el documento que se ha firmado, quienes son los firmantes, una declaración de que el sello de tiempo se aplicará usando GMT, etcétera. Además, el solicitante genera las credenciales necesarias y la información 214 de identificación que se usarán por el dispositivo 90 para autorizar la solicitud y para asegurar que se usa el reloj virtual correcto.

En 216, las credenciales 214, la cabecera 212 y el mensaje de recopilación 208 son concatenados y son suministrados a la entrada 92.

Dentro del dispositivo, la credencial y la información 214 de control es extraída (tal como se ilustra esquemáticamente mediante las líneas 220 onduladas), dejando solo la cabecera 212 y el mensaje de recopilación 208 a presentar como una entrada a la sección 150 de firma. La otra entrada es un mensaje 211 de tiempo, tal como es suministrado por la sección 140 de compensación. Estas dos entradas son concatenadas y firmadas digitalmente, tal como se ha descrito anteriormente, usando la clave privada apropiada para ese reloj virtual particular. A continuación, el mensaje 230 de salida firmado y con sello de tiempo es puesto en la salida 94 del dispositivo.

Por supuesto, se entenderá que se puede firmar electrónicamente y se puede aplicar un sello de tiempo a cualquier tipo de datos o de documento digital.

REIVINDICACIONES

1. Dispositivo de sellado de tiempo para el sellado de tiempo digital de los datos de entrada, que comprende:

un temporizador (130) que tiene una salida de temporizador;

medios de firma adaptados para (150) generar una salida (94) con sello de tiempo

caracterizado por

los medios (120) de memoria adaptados para almacenar una pluralidad de conjuntos de información (124) de calibración de temporizador, definiendo cada uno las características de un reloj virtual respectivo;

medios de compensación adaptados para (140) ajustar la salida del temporizador según un reloj virtual seleccionado por el usuario, para generar un salida del reloj virtual seleccionado; y

medios de firma adaptados para generar la salida con sello de tiempo dependiendo de la salida del reloj virtual seleccionado y los datos de entrada.

2. Dispositivo de sellado de tiempo según la reivindicación 1, en el que cada reloj virtual tiene asociado al mismo una clave (126) de firma respectiva, en el que los medios de firma adaptados para (150) generar la salida (94) con sello de tiempo usan la clave asociada con el reloj virtual seleccionado.

3. Dispositivo de sellado de tiempo según la reivindicación 2, en el que los medios (150) de firma están adaptados para concatenar la salida del reloj virtual seleccionado y los datos de entrada, y firma los datos concatenados resultantes.

4. Dispositivo de sellado de tiempo según la reivindicación 2 o la reivindicación 3, en el que cada clave (126) de firma comprende la parte privada de un par de claves pública/privada.

5. Dispositivo de sellado de tiempo según una cualquiera de las reivindicaciones 2 a 4, que incluye medios de control de acceso a clave adaptados para (110) autorizar solicitudes para operaciones de gestión de claves.

6. Dispositivo de sellado de tiempo según una cualquiera de las reivindicaciones anteriores, que incluye medios (100, 110) de control de acceso a sello de tiempo adaptados para autorizar solicitudes de usuario para el sellado de tiempo de los datos de entrada según una salida de reloj virtual determinado.

7. Dispositivo de sellado de tiempo según una cualquiera de las reivindicaciones anteriores, que incluye medios (110) de control de acceso a reloj virtual adaptados para autorizar solicitudes para modificar la información (124) de calibración para un reloj virtual determinado.

8. Dispositivo de sellado de tiempo según una cualquiera de las reivindicaciones anteriores, en el que el temporizador (130) es un temporizador de funcionamiento libre.

9. Dispositivo de sellado de tiempo según una cualquiera de las reivindicaciones 1 a 7, en el que el temporizador (130) está adaptado para recibir señales de temporización desde una fuente (134) externa.

10. Dispositivo de sellado de tiempo según una cualquiera de las reivindicaciones anteriores que comprende un módulo hardware.

11. Procedimiento de sellado de tiempo digital de los datos de entrada, que comprende:

seleccionar un conjunto de información (124) de calibración de temporizador de entre una pluralidad de dichos conjuntos, definiendo cada conjunto las características de un reloj virtual respectivo;

ajustar una salida de temporizador según el conjunto seleccionado para generar una salida del reloj virtual seleccionado; y

firmar datos representativos de ambos la salida del reloj virtual seleccionado y los datos de entrada para generar una salida (94) con sello de tiempo.

12. Procedimiento según la reivindicación 11, en el que cada reloj virtual tiene asociado al mismo una clave (126) de firma respectiva, incluyendo el procedimiento generar la salida (94) con sello de tiempo usando la clave asociada con el reloj virtual seleccionado.

13. Procedimiento según la reivindicación 12, que incluye concatenar la salida del reloj virtual seleccionado y los datos de entrada, y firmar los datos concatenados resultantes.

14. Procedimiento según la reivindicación 12, en el que cada clave (126) de firma comprende la parte privada de un par de claves pública/privada.

15. Procedimiento según una cualquiera de las reivindicaciones 12 a 14, que incluye comprobar las credenciales de las solicitudes para las operaciones de gestión de claves.

16. Procedimiento según una cualquiera de las reivindicaciones 11 a 15, que incluye comprobar las credenciales de las solicitudes de usuario para el sellado de tiempo de los datos de entrada según una salida del reloj virtual determinado.

17. Procedimiento según una cualquiera de las reivindicaciones 11 a 16, que incluye comprobar las credenciales de las solicitudes para modificar la información (124) de calibración para un reloj virtual determinado.

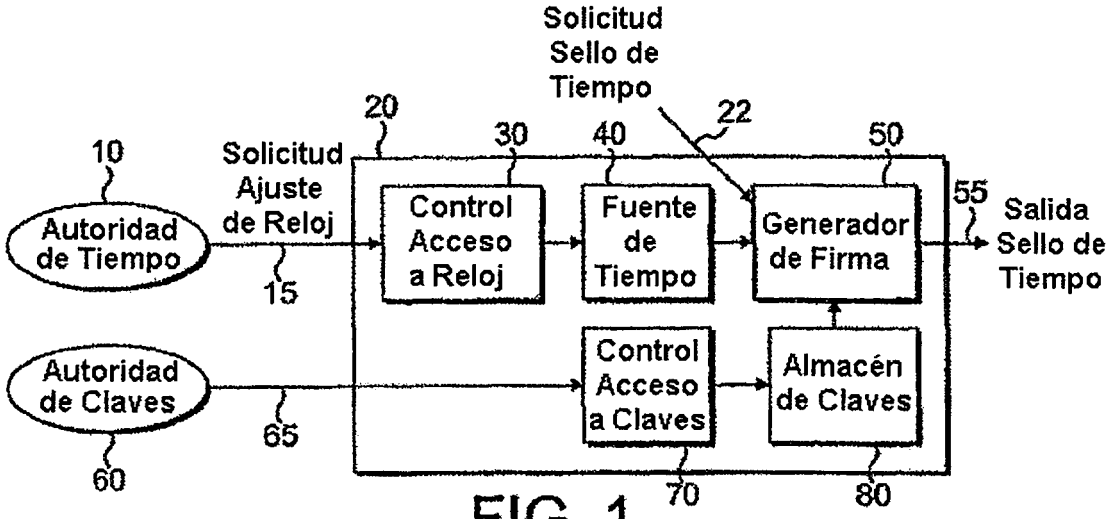

FIG. 1

TÉCNICA ANTERIOR

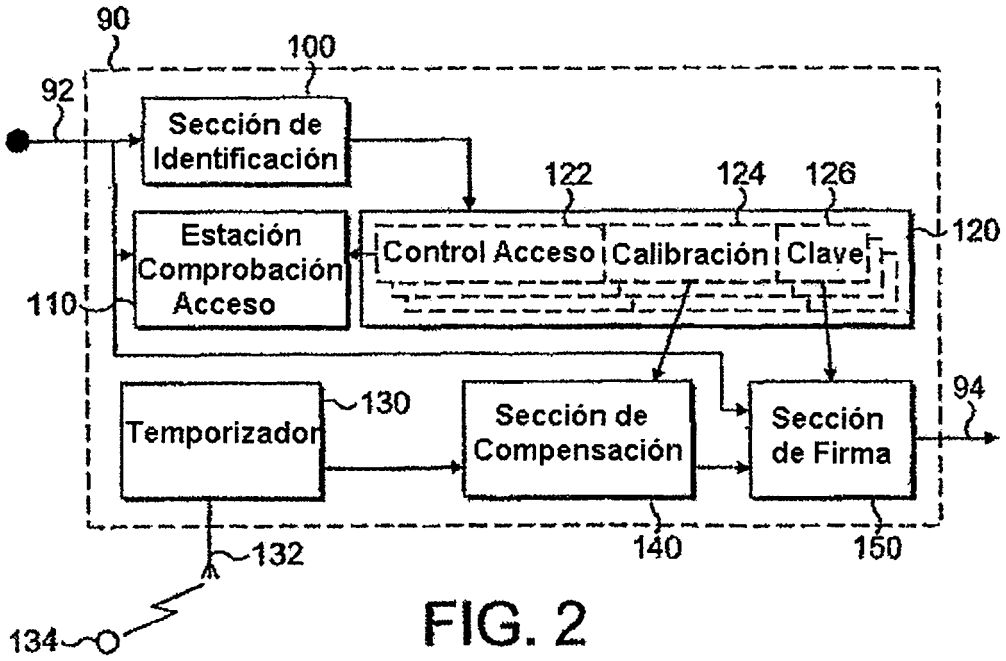

FIG. 2

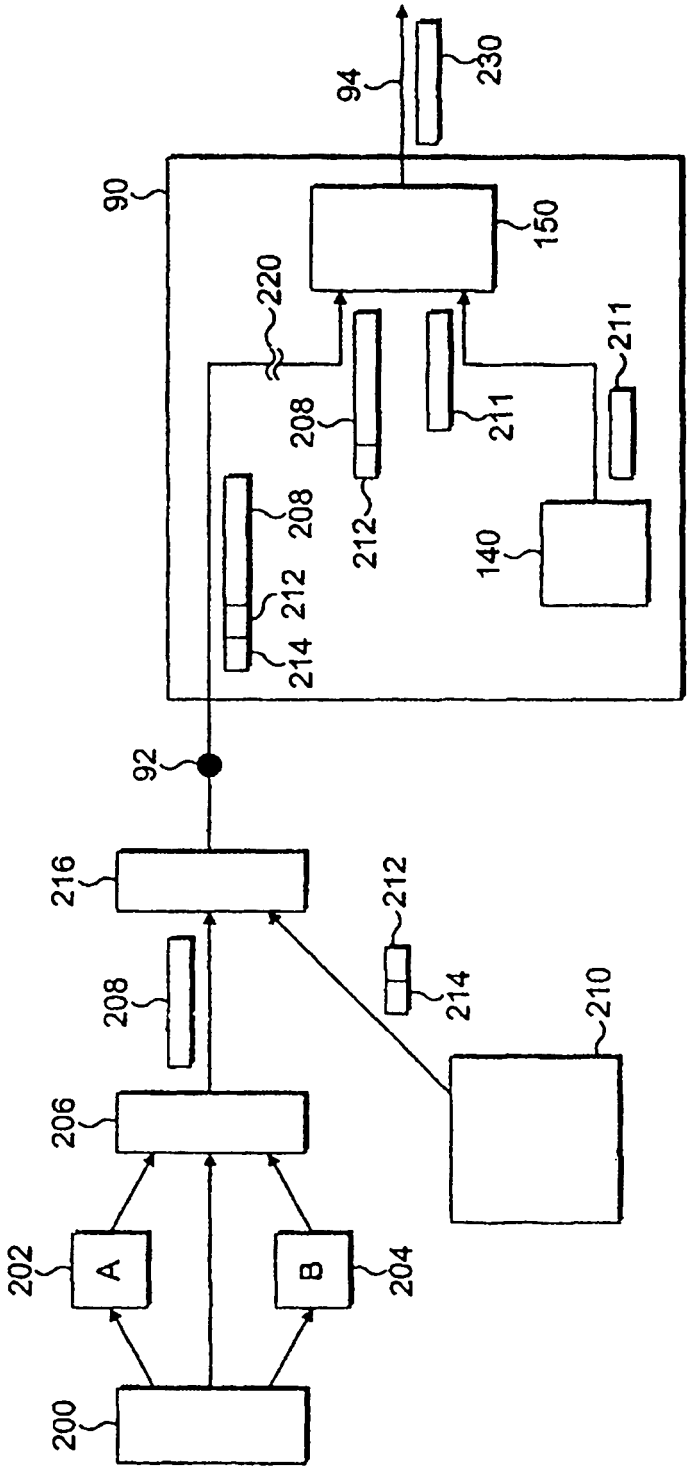
94
230
90
150
220
211
208
211
208
212
140
212
214
92
216
212
208
214
210
206
202
A
B
204
200

FIG.3