



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 265 189**

51 Int. Cl.:
G07B 17/00 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

- 86 Número de solicitud europea: **99958120 .0**
86 Fecha de presentación : **19.11.1999**
87 Número de publicación de la solicitud: **1131793**
87 Fecha de publicación de la solicitud: **12.09.2001**

54 Título: **Método y sistema para producir y verificar una marca de franqueo.**

30 Prioridad: **20.11.1998 NL 1010616**
10.02.1999 NL 1011270

45 Fecha de publicación de la mención BOPI:
01.02.2007

45 Fecha de la publicación del folleto de la patente:
01.02.2007

73 Titular/es: **PTT Post Holdings B.V.**
Prinses Beatrixlaan 23
2595 AK Den Haag, NL

72 Inventor/es: **Wesseling, Hennie;**
Brandt, Dick;
Van Halderen, Anthonius, Johannes, Franciscus;
Pieterse, Rob;
Van Golden, Niels, Alexander y
Gerlofs, Johannes, Francis

74 Agente: **Tomás Gil, Tesifonte-Enrique**

ES 2 265 189 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Método y sistema para producir y verificar una marca de franqueo.

La presente invención se refiere a un método para controlar una marca de franqueo, que al menos comprende un código de identificación y una secuencia de bits única.

“Marca de franqueo” se refiere aquí, por ejemplo, a un sello postal electrónico, es decir una marca impresa en un artículo postal por una máquina o una impresora de franqueo, que entre otras cosas puede representar un valor de franqueo para dicho artículo postal. En el contexto de la presente invención, no obstante, “marca de franqueo” tiene un significado amplio. El concepto “marca de franqueo” pueden aludir a todo tipo de marca que puede ser colocada en documentos arbitrarios para asegurar dichos documentos. Además de artículos postales, tales documentos pueden ser también documentos de valor, tales como entradas, resguardos de pago, etc., que son protegidos por tal marca.

Además de los detalles del proceso de control, la sustancia de la presente invención está descrita también en la solicitud de patente Holandesa 1010616, cuya prioridad se reivindica.

Se conoce el uso de sellos de franqueo electrónicos, por ejemplo, por los siguientes dos documentos públicamente descritos por el Centro de Ingeniería del Servicio Postal de Estados Unidos (USPS): “Information Based Indicia Program (IBIP), Open System Indicum Specification” e “Information Based Indicia Program (IBIP), Open System Postal Security Device (PSD) Specification”, ambos de fecha 23 de julio de 1997 (borradores).

Con este método se pueden obtener e imprimir sellos de franqueo electrónicos en artículos postales. El dispositivo, por ejemplo un ordenador, con el cual el sello postal electrónico es impreso está provisto para ello de un Dispositivo de Seguridad Postal (PSD del inglés Postal Security Device), al que se asocia un código de identificación única. El sello postal electrónico comprende varios elementos, de los cuales se mencionan algunos como “críticos para la seguridad”: el código de identificación del PSD, el valor del contenido de un registro incremental, el valor de franqueo del artículo postal y una firma digital. El contenido del registro incremental representa el valor monetario total de todos los sellos postales impresos hasta el momento con el PSD asociado. La combinación del código de identificación y el contenido del registro incremental representa una secuencia de bits única por artículo postal. Puesto que la manera en la que dicha secuencia de bits única es compuesta debe cumplir una regla conocida, puede predecirse el valor de una secuencia de bits única siguiente para un sello postal electrónico siguiente, lo cual es desventajoso con respecto a un posible fraude.

En un artículo de J. Quittner en FOX Market Wire de 9 de abril de 1998, “Neither bugs, nor hackers, nor Pitney Bows will keep E-stamp from delivering your postage”, disponible en internet el 5 de mayo de 1998, se describe tal sistema, que cumple estas especificaciones y es original de la empresa E-Stamp. El sistema de E-Stamp también usa un ordenador personal para imprimir una marca de franqueo en un artículo postal directamente con la ayuda de una impresora corriente conectada a dicho ordenador personal. El

ordenador personal está conectado, a través de internet, con el Servicio Postal de Estados Unidos. De este modo se pueden comprar a través de internet “sellos postales electrónicos” en el Servicio Postal de Estados Unidos. El valor de franqueo del sello postal electrónico es debitado directamente en el saldo de la cuenta del cliente asociado y almacenado y protegido en el PSD. El PSD es una pequeña caja que puede ser introducida en la parte posterior de una impresora láser corriente. En cuanto un usuario emite una orden para imprimir un sello postal electrónico en un artículo postal, se descarga un sello postal electrónico y la impresora imprime un código de barras bidimensional, después de lo cual el valor del “sello postal” impreso es debitado del valor de franqueo total en el dispositivo de seguridad postal.

En el sistema de E-Stamp, el sello postal electrónico según la publicación de J. Quittner comprende en todo caso un código de identificación del usuario, un código de identificación del dispositivo de seguridad postal, el valor de franqueo, el tipo de envío (por ejemplo envío urgente), la dirección del remitente y la fecha. Además, el sello postal electrónico puede también contener datos relacionados con la compañía de envío y se provee un espacio para posibles anuncios.

En la patente Americana US-A-5.666.284 de E-Stamp Corporation se describe un sistema y un método para imprimir un sello de franqueo postal, incluyendo una cantidad de franqueo deseado e información encriptada, sobre un artículo postal. En este sistema se crea un número único, que es usado para la validación, entre otros por un cliente suministrando información privada como dirección, código postal, número de la Seguridad Social etc. el número creado es enviado a una oficina central y almacenado. Cuando un artículo postal pasa el control de validación el número en el artículo postal es leído y comparado con el número único almacenado centralmente pero creado localmente.

En la solicitud de patente europea EP-A-0 854 444 de Pitney-Bowes, se describe un método para controlar claves usadas en la verificación de información codificada que es impresa en un documento. El método usa testigos de autenticación postales únicos, generados en máquinas de franqueo, donde las secuencias de bits de los testigos de autenticación postales dependen de datos postales y la máquina de franqueo que se usa.

En la solicitud de patente europea EP-A-0 331 352 de Alcatel, se describe un método de franquear artículos postales en el que la impresión de franqueo incluye una parte legible por una máquina y una parte visualmente legible. La parte legible por la máquina comprende bloques de datos que incluyen un número pseudo-aleatorio que es encriptado antes de la impresión. Los números pseudo-aleatorios son generados por las máquinas de franqueo. La parte legible por la máquina es leída en un centro de gestión postal para proporcionar una entrada a una función postal de carga y contabilidad.

En la solicitud de patente europea EP-A-0 710 930 de Pitney-Bowes, se describe un sistema de tratamiento de correo con autorización única del artículo postal asignada previamente a los artículos postales que entran en una corriente de procesamiento de un servicio de transporte postal. En este sistema, un remitente envía un fichero postal al servicio de transporte. El transportista genera identificadores únicos del artículo postal a los artículos postales en el fichero postal,

y manda un fichero de identificación postal al remitente. El identificador único es luego impreso en el artículo postal. Los artículos postales son luego enviados al servicio de transporte, que obtiene el identificador único impreso del artículo postal. El identificador único obtenido se utiliza para verificar aquellos datos asociados al artículo postal que ha sido procesado por el transportista.

El objetivo de la presente invención es proveer un método y un sistema que pueda controlar tales sellos postales electrónicos.

Este objeto es conseguido por el método según la reivindicación 1 y el sistema según la reivindicación 10.

La presente invención será explicada a continuación con referencia a algunos dibujos destinados a ser sólo una ilustración de la invención y no una limitación de la misma. En particular, la invención tiene una aplicación más amplia que solamente el tráfico postal.

La Fig. 1 muestra una forma de realización de un sistema según la invención, donde se usa un soporte de información en el que uno o más sellos postales electrónicos pueden ser almacenados;

La Fig. 2a muestra las fases de un método para proveer un sello postal electrónico;

Fig. 2b muestra las fases de un método para proveer el sello postal electrónico, donde se usa un contador;

La Fig. 3a muestra las fases para imprimir un sello postal electrónico;

La Fig. 3b muestra las fases para imprimir un sello electrónico, donde se usa un contador;

Las Figs. 4a y 4b muestran las fases de un método según la invención donde se usa un ordenador personal;

La Fig. 5 muestra un sistema según la invención, donde se usa un ordenador personal;

La Fig. 6 muestra de forma esquemática un proceso de clasificación para artículos postales;

La Fig. 7 muestra algunos elementos para controlar una marca de franqueo;

Las Figs. 8 a 14 inclusive muestran flujogramas que ilustran mejor el proceso de control.

En la Fig. 1, el número de referencia 2 se refiere a un terminal, que, por ejemplo, se fija en la pared de una oficina postal. Dicho terminal 2 puede comunicar con una central 34, por ejemplo por medio de la red telefónica pública conmutada (PSTN del inglés Public Switched Telephone Network) 46. Evidentemente son posibles otras vías de comunicación por medio de otras redes. En este caso, se puede usar internet. La comunicación puede también tener lugar de otras formas, por ejemplo por medio de CDROMs, disquetes, etc.

El terminal 2 mostrado en la Fig. 1 comprende un procesador 4, que es acoplado a un medio de visualización 8 para comunicar con un usuario. Dicho terminal 2 también comprende una memoria 6, que es conectada a dicho procesador 4. El número de referencia 10 se refiere de forma esquemática a un teclado, con el cual un usuario puede introducir datos e instrucciones a dicho procesador 4. Para ello, dicho teclado 10 está conectado a dicho procesador 4. Dicho procesador 4 está conectado además a un Módulo de Acceso/ Aplicación Seguro 3 (normalmente llamado "SAM" del inglés Secure Access/Application Module). El SAM 3 es mostrado en la Fig. 1 dentro del terminal 2. Si se desea, el SAM 3 puede estar también

presente fuera del terminal 2. Si se desea, el SAM 3 puede incluso ser montado cerca o en la central 34.

En la forma de realización mostrada en la Fig. 1, dicho terminal 2 está provisto de dos unidades de entrada/salida 12, 14. En dicha unidad de entrada/salida 12, se puede introducir una tarjeta bancaria o una tarjeta de cajero automático. Para ello la unidad de entrada/salida 12 está provista de uno o más conectores adecuados (no mostrados) que pueden ponerse en contacto con la tarjeta bancaria y/o de cajero automático 16, como sabrán los expertos en la materia. Con una tarjeta bancaria y/o de cajero automático tal, el usuario puede identificarse y efectuar un pago a través del PIN. En el caso de que dicha tarjeta bancaria/de cajero automático contenga un monedero electrónico, el usuario puede efectuar también acciones de pago con ella, por ejemplo el pago de un sello postal electrónico que debe ser impreso en un artículo postal.

Dicha unidad de entrada/salida 14 está dispuesta para aceptar un soporte de información 18, que puede ser una tarjeta inteligente. Para ello, dichos medios de entrada/salida 14 son provistos de uno o más conectores adecuados que pueden ponerse en contacto con el procesador (no mostrado) en dicha tarjeta inteligente 18, como sabrán los expertos en la materia. En un soporte tal de información 18 son almacenados uno o más sellos postales electrónicos. Tales sellos postales son luego preferiblemente almacenados bajo la protección de un código de autenticación de mensajes (MAC del inglés Message Authentication Code) y/o protección por codificación.

La tarjeta de cajero automático/bancaria es una tarjeta inteligente de múltiples funciones, que entre otras cosas puede ser usada para pagar, pero también ofrece posibilidades para otras aplicaciones. Un ejemplo de tal tarjeta inteligente es la Chipper[®] de la KPN Telecom y el Postbank de Holanda. En este caso, dichas tarjetas 16 y 18 pueden ser la misma tarjeta y dichos medios de entrada/salida 12 pueden ser omitidos.

Alternativamente, dicho soporte de información 18 también puede ser una tarjeta con, por ejemplo, una banda magnética que en sí misma no esté provista de un medio procesador. Los datos pueden después ser escritos en, leídos y borrados de la banda magnética por dicho terminal 2. En este caso, los sellos postales electrónicos pueden ser almacenados bajo protección por codificación. Es imaginable que dicho terminal 2 tenga un suministro de tales tarjetas de banda magnética y que un cliente compre una o más de tales tarjetas. En la banda magnética se pueden almacenar entonces uno o más de tales sellos postales electrónicos. Tales tarjetas de banda magnética pueden ser tarjetas desechables. Opcionalmente también se pueden usar tarjetas de chip como tarjetas desechables.

En la Fig. 1, el número de referencia 20 se refiere a una máquina de franqueo. Dicha máquina de franqueo 20 está provista de medios de entrada/salida 21 para aceptar dicho soporte de información 18. Dicha máquina de franqueo 20 está también provista de un procesador 23, que, además de estar conectado a dichos medios de entrada/salida 21, también está conectado a un medio de pesado 25, una impresora 27 y un SAM 19.

Por medio de dichos medios de entrada/salida 21, dicho procesador 23 puede comunicar con el soporte de información 18.

Con la ayuda del medio de pesado 25, la máquina

de franqueo 20 puede determinar el peso de un artículo postal 22.

Con la ayuda de dicha impresora 27, la máquina de franqueo 20 puede posteriormente imprimir información 29 en el artículo postal 22.

Dicha información 29 comprende, por ejemplo, datos legibles por un humano 24 relacionados con la organización remitente (u otra publicidad), al igual que un signo de marcado 26 (por ejemplo un código de barras) permitiendo la orientación automática del artículo postal en una máquina de sellado/clasificación, y una marca de franqueo 28, por ejemplo en forma de un código de barras bidimensional 28, conteniendo además información, posiblemente codificada. Dicha marca de franqueo 28 al menos contiene una secuencia de bits única, cuyo uso se explicará más adelante, y un código de identificación. El código de identificación identifica al usuario, es decir a la persona que compra el sello postal electrónico, y/o el dispositivo con el cual se imprime la marca de franqueo. Si el código de identificación está asociado al dispositivo de impresión, este puede, por ejemplo, ser un código único en relación con dicho SAM 19. En este caso, el propietario de la máquina de franqueo es responsable del posible fraude con el uso de sellos postales electrónicos.

Como código de identificación del usuario se puede usar el número de dicha tarjeta bancaria 16. El número de tarjeta bancaria es después de todo un número único que está asociado al usuario, proporcionando un grado razonable de certeza de que el usuario es el propietario de dicha tarjeta bancaria 16 al hacer que él mismo se identifique por medio de un código PIN.

Además, dicha marca de franqueo 28 puede comprender información relacionada con el terminal 2 y la máquina de franqueo 20, al igual que el tipo de envío postal (ordinario, envío urgente, certificado, por correo aéreo, etc.).

El valor de franqueo puede también ser impreso en el artículo postal 22 de una forma legible por un humano 31.

En dicho artículo postal 22, se asigna un espacio para la dirección 30 del destinatario.

El sistema mostrado en la Fig. 1 comprende un dispositivo 32 para leer dichos artículos postales 22 durante el despacho desde el remitente hasta el destinatario. Si la secuencia de bits única representa directamente un valor de franqueo, el valor de franqueo, por ejemplo, puede ser controlado. Los datos leídos por dicho dispositivo 32 pueden ser suministrado a la central 34. La información que es leída por dicho dispositivo 32 puede ser suministrada a dicha central 34 de cualquier manera según la técnica anterior.

Para introducir la información a un procesador 36 presente en dicha central 34, dicha central 34 está provista de un medio de entrada adecuado 44 que está conectado a dicho procesador 36.

Para llevar a la práctica el método según la invención, dicha central 34 está preferiblemente provista de tres memorias 38, 40, 42. Evidentemente no se requiere que éstas sean memorias separadas físicamente. Éstas pueden aludir a campos diferentes dentro de una memoria más grande.

La Fig. 2a muestra una forma de realización posible del funcionamiento del terminal 2 durante la operación.

Un cliente llega a dicho terminal 2 e introduce su tarjeta bancaria 16 (esta se usará de ahora en adelante

para aludir tanto a una tarjeta bancaria/de cajero automático o cualquier tarjeta inteligente (de múltiples funciones)) en el medio de entrada/salida correspondiente 12. El procesador 4 pregunta, a través del monitor 8, qué tipo de sellos postales electrónicos desea tener el cliente. El cliente puede, por ejemplo, indicar que desea comprar una tarjeta de franqueo 18 (se usará este término de ahora en adelante para cualquier tipo posible de soporte de información 18) con 100 sellos postales electrónicos de 80 céntimos. Esto tiene lugar en el fase 202.

El procesador 4 lee el número de la tarjeta bancaria 16 y pide al usuario que se identifique con su código PIN, fases 204 y 206.

En la fase 208, dicho procesador 4 verifica, de manera conocida *per se*, si el cliente se ha identificado correctamente. Si no, sigue un mensaje de error en la fase 210. Tras el mensaje de error de la fase 210, dicho procesador 4 puede volver al principio del flujo representado en la Fig. 2a. Alternativamente se le pueden dar tres oportunidades al usuario, como se conoce *per se*, para que introduzca el código PIN correcto.

Si un usuario se identifica correctamente, el programa en dicho procesador 4 salta a la fase 212 y lee un número de franqueo. Según la invención, el número de franqueo consiste en una secuencia de bits que es única y es seleccionada de un grupo de secuencias de bits únicas.

El grupo de secuencias de bits únicas es almacenado en dicha memoria 38 en dicha central 34. Dicha central 34 está conectada a varios terminales 2 distribuidos por el país y puede, por ejemplo por medio de la red PSTN 46, facilitar uno o más números de franqueo únicos del grupo de números de franqueo únicos a dichos terminales 2. En este caso, una cierta cantidad deseada de números de franqueo únicos pueden ser transferidos por transacción desde la memoria 38 de la central 34 hacia la memoria 6 del terminal 2. Alternativamente, no obstante, cada uno de los terminales 2 puede tener almacenado un determinado suministro de números de franqueo únicos en dicha memoria 6 previamente, de manera que no se requiera establecer una conexión entre el terminal 2 y la central 34 cada vez que tenga lugar una transacción con un cliente. La transmisión de las secuencias de bits únicas pueden ser protegidas de cualquier manera según la técnica anterior.

El grupo de números de franqueo únicos en la memoria 38 de la central 34 consiste, por ejemplo, en secuencias de bits de 128 bits. Este grupo contiene así tal cantidad de números de franqueo únicos que cubrirá la necesidad de tales números durante años.

Preferiblemente antes de la fase 212, el cliente paga la tarjeta de franqueo 18 de una manera electrónica. Esto se hace con la ayuda de la tarjeta bancaria 16 de una manera conocida *per se*. Es decir que, si dicha tarjeta bancaria 16 es una tarjeta bancaria corriente, el pago se produce debitando el saldo bancario del cliente. La manera en la que esto se hace es conocida por los expertos en la materia y no requiere ser explicada aquí con más detalles. En el caso de que dicha tarjeta bancaria 16 comprenda un monedero electrónico, la cantidad debida puede ser debitada directamente del saldo de dicha tarjeta bancaria 16. El pago se puede realizar también en efectivo.

El procesador 4 entonces provee, por medio del medio de entrada/salida 14, una tarjeta de franqueo

separada 18 donde tanto el código de identificación como el número de franqueo asociado están almacenados. Dicho código de identificación y dichos números de franqueo son almacenados con un código de autenticación de mensaje MAC1, que es calculado por el SAM 3 del terminal 2 con el procesador de la tarjeta bancaria 16. Como se sabe, un MAC es una suma de control de un texto suministrado mediante la cual se puede controlar si el texto suministrado es válido. Cada modificación en el texto (en este caso el código de identificación y los números de franqueo) puede ser detectada. Un MAC sólo puede ser calculado con una clave secreta, que sólo conoce dicho SAM 3 y las autoridades postales adecuadas. La generación del MAC1 y el almacenamiento de los datos requeridos en la tarjeta de franqueo 18 se producen en las fases 214 y 216.

Si se facilitan varios números de franqueo para usar, el cálculo de otros tantos MAC1 puede requerir demasiado tiempo. En consecuencia, según se desee, el cálculo del MAC1 puede limitarse a un cálculo sobre el código de identificación y/u otros datos conocidos tales como fecha de emisión, valor etc.

Como alternativa para el cálculo de un MAC, los datos pueden ser almacenados también de forma codificada.

Para una mayor protección del conjunto, el procesador 4 manda preferiblemente una copia del código de identificación con los números de franqueo emitidos, protegidos por el MAC1 y/o protegidos por codificación, hacia la central 34, que almacena esta información en la memoria 40 de modo que se pueda controlar centralmente un posible fraude en una fase posterior, fase 218. Esto se explicará con mayor detalle más adelante.

Si se desea, se puede almacenar un código de terminal, que identifique únicamente al terminal 2 que expidió la tarjeta de franqueo 18, en la memoria de la tarjeta de franqueo 18. Si se desea, dicho código de terminal puede formar parte del cálculo que el MAC1 ha suministrado. El código de terminal, concretamente, tampoco puede ser cambiado después de forma inadvertida.

La Fig. 3a muestra un flujograma del funcionamiento de la máquina de franqueo 20 según el método explicado en relación a la Fig. 2a.

Un usuario introduce su tarjeta de franqueo 18 en el medio de entrada/salida 21 de la máquina de franqueo 20 destinado para ello. Al hacer esto, se establece contacto entre la tarjeta de franqueo 18 y el procesador 23 de la máquina de franqueo 20. A través de un medio de introducción adecuado (por ejemplo un teclado, no mostrado), el usuario envía una orden a dicho procesador 23 para imprimir un sello postal electrónico en el artículo postal 22. Tan pronto como dicho procesador 23 ha establecido que tal instrucción ha sido recibida, fase 302, dicho procesador 23 lee o bien el MAC1 con el código de identificación asociado y el número de franqueo, o bien el código de identificación y el número de franqueo de forma codificada de dicha tarjeta de franqueo 18. En caso de que esté presente, también se leerá el código de terminal que está almacenado en dicha tarjeta de franqueo 18.

En base a los datos leídos, la máquina de franqueo 20 compone, de una manera predeterminada, una marca de franqueo y la imprime en el artículo postal 22, fase 306. Para ello, dicha máquina de franqueo 20, de una manera conocida *per se*, está provista

de una abertura donde el artículo postal 22 puede ser introducido, de modo que la marca de franqueo pueda ser impresa en el artículo postal 22 con la ayuda de la impresora 27.

La situación puede ser tal, por ejemplo, que dicho procesador 23 sea capaz de controlar si el valor de franqueo es suficiente en vista del peso de dicho artículo postal 22. Para ello, dicho artículo postal 22 es pesado por el medio de pesado 25, que envía una señal de pesado a dicho procesador 23. El número de franqueo puede, por ejemplo, pertenecer a un subgrupo determinado de todos los números de franqueo únicos que sólo pueden ser utilizados para artículos postales de hasta 50 gramos inclusive. Entonces se proporciona un subgrupo separado de números de franqueo únicos por clase de peso y por tipo de envío postal. Dicho procesador 23 puede controlar así directamente si el valor de franqueo es correcto, y, si este no fuera el caso, advertir al usuario por medio de un monitor (no mostrado).

La marca de franqueo, por ejemplo, es impresa en forma de un código de barras bidimensional 28 en el artículo postal 22. Preferiblemente la marca de franqueo comprende al menos los siguientes datos: el número de franqueo asociado, el código de identificación del usuario, el código de terminal del terminal 2 y un código de la máquina de franqueo que identifica la máquina de franqueo 20. Preferiblemente dichos datos, provistos de otro MAC (MAC2), son impresos en la marca de franqueo. Tal MAC2 es calculado por el SAM 19 en la máquina de franqueo 20 con la tarjeta de franqueo 18, por lo cual ésta debe ser provista de un procesador (no mostrado). Alternativamente, los datos pueden también ser impresos de forma codificada, en cuyo caso la codificación tiene lugar con la ayuda de técnicas criptográficas conocidas (posiblemente incluyendo la colocación de una firma digital). Si se desea, el SAM 19 puede seguir el control de un contador que, a partir de un momento determinado en el tiempo t_0 , refleje la cantidad total consumida de franqueo en la máquina de franqueo 20 hasta el momento concernido. El contenido de este contador entonces también forma parte de la marca de franqueo.

Opcionalmente, la marca de franqueo 28 puede también comprender: Información de dirección del destinatario y remitente (posiblemente dirección de devolución), información del servicio tal como "certificado", "envío urgente", etc., y fecha y hora. Esta información puede después ser provista de un MAC y/o ser codificada con los datos mencionados arriba con la ayuda de técnicas criptográficas conocidas.

Una vez que la máquina de franqueo 20 haya impreso la marca de franqueo en el artículo postal 22, dicha máquina de franqueo 20 puede hacer imposible cualquier uso posterior del número de franqueo usado en la tarjeta de franqueo 18. Esto se produce en la fase 308. Esto se puede hacer, por ejemplo, borrando el número de franqueo asociado a dicha tarjeta de franqueo 18.

Tras el despacho del artículo postal 22 desde un remitente hasta un destinatario, dicho artículo postal 22, en un momento dado, llega a un centro de clasificación. Allí dicho artículo postal 22 será leído con la ayuda de los medios 32, y se puede controlar nuevamente si dicho artículo postal 22 ha sido suficientemente franqueado. Los medios 32 leen al menos la marca de franqueo 28. Los medios 32 recogen así todas las marcas de franqueo leídas 28 de todos los artí-

culos postales que están provistos de ellas. Todas las marcas de franqueo 28 son posteriormente enviadas a la central 34 y allí son leídas por el procesador 36 por medio del medio de entrada 44. Dicho procesador 36 almacena las marcas de franqueo introducidas en la memoria 42.

En una fase anterior, dicho procesador 36 ya ha recibido los datos de los terminales 2 asociados bien a los números de franqueo expedidos con los códigos de identificación asociados y MAC1, o a los números de franqueo codificados con los códigos de identificación asociados. Dichos datos fueron almacenados en la memoria 40 por el procesador 36. Así dicho procesador 36 es capaz de comparar los datos recibidos a través del medio de entrada 44, después del almacenamiento en la memoria 42, con los datos almacenados en dicha memoria 40. Así se puede controlar si los números de franqueo presentes en dicha memoria 42 fueron realmente emitidos. Si el número de franqueo, el código de identificación, el código de terminal y/o el código de la máquina de franqueo han sido alterados de cualquier manera, dicho procesador 36 puede encontrarlo directamente desde el MAC1 y MAC2 o los datos codificados incluidos en la marca de franqueo. Dicho procesador 36 puede luego encontrar además las irregularidades de usuario que han tenido lugar y para qué terminal 2. El código de identificación, después de todo, únicamente identifica el usuario y/o el SAM 3 en el terminal 2.

Otro control tiene lugar a través del procesador 36 manteniendo aquellos números de franqueo únicos que fueron enviados a los terminales 2, por ejemplo almacenando dichos números de franqueo en la memoria 40. Evidentemente dichos números de franqueo pueden también ser almacenados en otra memoria. En primer lugar, dichos números de franqueo que ya fueron enviados a los terminales 2 no pueden volver a ser enviados después. En segundo lugar, los datos enviados a la central 34 por los terminales 2 pueden entonces, en una primera vuelta, ser ya comparados con los números de franqueo emitidos, de modo que se pueda controlar directamente si los números de franqueo emitidos por los terminales 2 fueron realmente números de franqueo que fueron enviados desde la memoria 38.

Si la marca de franqueo 28 posee un código de identificación que únicamente identifica el propietario de la tarjeta bancaria 16, es posible implementar la invención con pago diferido. Después de todo, cuando recibe las marcas de franqueo 28 el procesador 36 puede inequívocamente encontrar qué clientes han usado qué números de franqueo. Esto abre la posibilidad de que los medios 32, por ejemplo, midan el peso del artículo postal 22 e informen a dicho procesador 36 del peso con la marca de franqueo 28. En este caso, dicho procesador 36 establece entonces cuánto debe pagar el cliente para enviar el artículo postal asociado, el uno y el otro dependiendo de, por ejemplo, el peso del artículo postal 22 y el tipo de despacho. Entonces se debita el saldo bancario del cliente por la cantidad correspondiente de una manera conocida *per se*. Evidentemente en lugar de esto se puede enviar una factura o se puede debitar el saldo en otro banco, con el que, de una manera conocida *per se*, se establece un vínculo de comunicación. La ventaja de este método alternativo es que la emisión de números de franqueo ya no está asociada al valor que es requerido en vista del peso y el tipo de

despacho de dicho artículo postal 22. El número de franqueo único es pues sólo una identificación del artículo postal 22. El número de franqueo no necesita comprender información relacionada con el valor de franqueo.

Por ello, en teoría, son posibles dos tipos de tarjetas: tarjetas recargables (por ejemplo tarjetas inteligentes) y tarjetas no recargables (por ejemplo tarjetas de banda magnética). En teoría, también son posibles tres formas diferentes de pago en ambos casos: prepago total de cada sello postal electrónico, pago diferido total de cada sello postal electrónico, y una combinación de prepago y pago diferido de sellos postales electrónicos.

Las Figs. 2b y 3b muestran flujogramas para una forma de realización alternativa del método según la invención. Dicho método alternativo se refiere a una forma de realización en la que no se aplica un número de franqueo único por artículo postal. En algunos casos, un cliente podría desear franquear 1000 o más artículos postales, por ejemplo. Con los medios disponibles actualmente para almacenar datos en tarjetas de crédito y/o tarjetas provistas de bandas magnéticas, es imposible almacenar tales cantidades grandes de números de franqueo únicos, constando, por ejemplo, de 128 bits. Este problema puede ser sorteado suministrando un número de franqueo con un cierto valor de contador.

El método para suministrar un sello electrónico con contador es explicado en base a la Fig. 2b. La fase 252 corresponde a la fase 202 en la Fig. 2a.

La fase 254 muestra de forma abreviada que un usuario debe identificarse, por ejemplo de la manera explicada en base a las fases 204-210 en la Fig. 2a.

La fase 256 corresponde a la fase 212 de la Fig. 2a.

Una vez que el procesador 4 ha leído el número de franqueo, dicho procesador 4, en la fase 258, lee un valor de contador. Dicho procesador 4 pueden hacer esto, por ejemplo, pidiendo al usuario por medio del monitor 8 que introduzca tal valor de contador. La magnitud del valor de contador entonces determina el número de veces que el número de franqueo asociado puede ser usado. Alternativamente, el contador puede representar un valor monetario que puede ser gastado en sellos postales electrónicos. El usuario puede introducir el valor de contador por medio de las teclas del teclado 10.

En la fase 260, dicho procesador 4 genera el MAC1 basándose en el código de identificación del usuario, el número de franqueo emitido y el valor de contador. Alternativamente, dichos datos pueden ser almacenados de forma codificada. El valor de contador, en consecuencia, es luego almacenado de modo seguro y no puede ser cambiado sin que pase inadvertido.

En la fase 262, dicho procesador 4 almacena bien el MAC1 con el código de identificación, el número de franqueo emitido y el valor de contador, o los datos codificados, en la tarjeta de franqueo 18.

Nuevamente, dicha tarjeta de franqueo 18 puede ser tal como se ha explicado arriba con referencia a la Fig. 2a.

En la fase 264, el procesador 4 manda una copia del MAC1 con el código de identificación, número de franqueo y valor de contador, o la forma codificada de dicho datos, a la central 34. La central 34 nuevamente almacena los datos en la memoria 40 y así sabe

cuántas veces se puede usar el número de franqueo asociado.

La Fig. 3b muestra un flujograma de la máquina de franqueo 20 para la forma de realización en la que se usa un contador.

En la fase 352, la máquina de franqueo 20 espera hasta que el cliente envíe una orden de imprimir un sello postal electrónico. Dicha fase corresponde a la fase 302 de la Fig. 3a.

Tan pronto como el cliente ha enviado esta orden, la máquina de franqueo lee bien el MAC1 con el código de identificación, número de franqueo y valor de contador, o dichos datos de forma codificada, de la tarjeta de franqueo 18. Esto se produce en la fase 354.

En la fase 356, el procesador 23 verifica si el valor de contador leído es aún superior a cero. Si este no es el caso, no se permite que se siga usando el número de franqueo asociado y sigue un mensaje de error en la fase 358. Después de la fase 358, el programa vuelve a la fase 352.

Si el valor de contador es por el contrario superior a cero, el programa del procesador 23 procede con la fase 360. En la fase 360, dicho procesador 23 controla la impresora 27 de tal manera que la marca de franqueo calculada por dicho procesador 23 sea impresa en el artículo postal 22. Dicha marca de franqueo es nuevamente preferiblemente provista del MAC2. Alternativamente, todos los datos son impresos de forma codificada en la marca de franqueo.

Luego, en la fase 362, el procesador 23 deduce el valor de contador en la tarjeta de franqueo 18 para indicar que el número de franqueo único asociado puede ser usado una vez menos, o deducir el valor disponible.

Evidentemente el cálculo del MAC2 también tiene en cuenta el valor de contador modificado.

El valor de contador real entonces forma parte de la marca de franqueo 28 en el artículo postal 22.

Cabe observar que la combinación de número de franqueo único y el valor de contador real conlleva aún una secuencia de bits única. Este secuencia de bits última, no obstante, tiene más bits que el número de bits del número de franqueo único.

El valor de contador vigente es entonces leído conjuntamente por los medios 32, y posteriormente también almacenados en la central 34, a través del medio de entrada 44 con la ayuda del procesador 36, en la memoria 42. Dicho procesador 36 entonces tiene la posibilidad de controlar si cada combinación de número de franqueo y valor de contador ha sido usada realmente sólo una vez. Puesto que la información asociada está protegida por el MAC2 o está almacenada de forma segura por codificación, el procesador 36 puede detectar la modificación ilícita de estos números.

Dicho procesador 36 puede también controlar si el cliente ha usado el número de franqueo el número de veces permitido.

Resultará evidente que la forma de realización según las Figs. 2b y 3b, así como la forma de realización según las Figs. 2a y 3a, pueden ser usadas con pago por anticipado o diferido.

Opcionalmente es posible, en la forma de realización según la Fig. 1, en la que se utiliza la tarjeta de franqueo 18, restringir el uso de la tarjeta de franqueo 18 a un número de máquinas de franqueo 20 predefinido. Para ello, las tarjetas de franqueo 18 pueden ser provistas de estos códigos de máquina de fran-

queo, asociados a dichas máquinas de franqueo 20, en las que se permite el uso de dicha tarjeta de franqueo 18.

Otra opción es implementar el sistema mostrado en la Fig. 1 de manera que se le asigne a cada una de las tarjetas de franqueo 18 un número único. Entonces se puede identificar un posible fraude con tarjetas de franqueo 18. La información asociada a dichas tarjetas de franqueo 18 usadas fraudulentamente puede después ser incluida en una tarjeta de franqueo arbitraria 18. Posteriormente, dicha información, asociada a las tarjetas de franqueo 18 usadas fraudulentamente, puede después ser transferidas "de forma desapercibida" a las máquinas de franqueo 20, que almacena la información asociada en una memoria (no mostrada). Si un cliente con tarjeta de franqueo 18 usada fraudulentamente desea imprimir un sello postal electrónico, la máquina de franqueo 20 puede detectar la tarjeta de franqueo relacionada 18 e invalidarla. Esto puede hacerse bien borrando el contenido de la tarjeta de franqueo 18 o haciéndolo ilegible, o simplemente rechazando imprimir un sello postal electrónico. De ese modo se pueden reducir otros daños por posible fraude.

Como alternativa al uso de un contador, también se puede utilizar un número de franqueo, que por ejemplo pueda ser usado por el cliente durante un número predeterminado de días. Esto es sólo posible en la forma de realización con la que tiene lugar el pago diferido. En este caso, el número de franqueo es además único, pero el número de franqueo se usa para más de un artículo postal 22. Puesto que en este caso se puede usar una tarjeta de franqueo 18 con un determinado número de franqueo único para un número indefinido de veces, es preferible aplicar en tal forma de realización un código PIN que necesite el usuario de la tarjeta de franqueo 18 para usar dicha tarjeta de franqueo 18 en la máquina de franqueo 20. En este caso, dicha máquina de franqueo 20 debe ser dispuesta de manera que pueda controlar el código PIN asociado a dicha tarjeta de franqueo 18.

La Fig. 5 muestra un ejemplo alternativo de la invención donde se usa un PC de un usuario en vez de un terminal 2 como se mostraba en la Fig. 1.

Las partes que son idénticas en las Figs. 1 y 5 tienen los mismos números de referencia.

En la Fig. 5, el número de referencia 52 designa el microprocesador del PC 50 de un usuario. El microprocesador 52 está conectado a un monitor 54, una impresora 62, un teclado 58 y, si se desea, un ratón 60. En un ejemplo, el microprocesador también está conectado a medios de entrada/salida 14, que pueden aceptar una tarjeta bancaria 18 (tarjeta chip de múltiples funciones). Para calcular el MACs o para determinar las codificaciones de los datos que deben ser impresos, el microprocesador 52 puede estar asociado a un SAM 64.

El microprocesador 52 está conectado, por ejemplo por medio de la red PSTN, a un sistema de servidor 70 para que diferentes sistemas informáticos puedan ser conectados. Se pueden proveer diferentes sistemas de servidor, cada uno con su propia conexión a los PC. Dicho sistema de servidor 70 está conectado a la central 34. Dicho sistema de servidor 70 comprende un procesador de servidor 72, al que se conecta un SAM o HSM (= Módulo de seguridad Huésped = un sistema informático con la misma funcionalidad que un SAM, pero con mucha más capacidad) 74.

La comunicación entre dicho PC 50 y el sistema de servidor 70 puede, por ejemplo, producirse con un protocolo de internet (IP).

La Fig. 4a muestra un flujograma de una forma de realización del funcionamiento del PC 50 en el contexto de la presente invención para recargar una tarjeta bancaria 18 con una cantidad deseada determinada para ser consumida en sellos electrónicos. La Fig. 4b se refiere a la impresión real de tal sello electrónico con tal tarjeta bancaria 18.

En la fase 402, el microprocesador 52 espera hasta que un usuario envíe una orden de suministrar una cantidad para uno o más sellos postales electrónicos. Para ejecutar tal petición, el usuario hace uso del medio de introducción conocido, tal como un teclado 58 y/o ratón 60. A este respecto, el usuario primero introduce su tarjeta bancaria 18 en la unidad de entrada/salida 14.

El microprocesador 52, por medio del monitor 54, pide al usuario que se identifique de una manera única, fase 404. Esto puede hacerse, por ejemplo, por la introducción por parte del usuario de su tarjeta bancaria 18 en el medio de entrada/salida 14, de modo que el microprocesador 52 pueda leer el número de dicha tarjeta bancaria 18. Posteriormente el usuario deberá identificarse, por ejemplo con la ayuda de un código PIN, para dejar claro que él es el usuario legítimo de dicha tarjeta bancaria 18. El control del código PIN preferiblemente se produce, como es conocido en la técnica anterior, en la propia tarjeta bancaria 18. Dicho microprocesador 52 puede posteriormente asumir que el usuario ha sido identificado de una manera única con la ayuda del número de tarjeta bancaria, por ejemplo. Esto se produce en la fase 404. Alternativamente, el microprocesador 52 pueden pedir al usuario que introduzca la combinación de número de tarjeta bancaria y PIN, u otra combinación única, por medio del teclado 58, después de lo cual estos datos son controlados localmente por el PC 50. En este caso, dicho PC 50 debe tener esta combinación de datos almacenada de forma segura.

En la fase 406, el microprocesador pide un número de franqueo único en la central 34. Esto ocurre de la misma manera como la que se explicó arriba con referencia a las Figs. 2a y 2b.

Posteriormente el SAM 74 del sistema de servidor 70, con la tarjeta bancaria 18, genera un MAC, MAC1 en base al código de identificación del usuario, el número de franqueo asociado y el saldo que se facilitó para los sellos electrónicos. Alternativamente, dicho sistema de servidor 70 calcula una codificación del código de identificación, el número de franqueo y dicho saldo. Este se produce en la fase 408.

En la fase 410, el microprocesador almacena, a elección, el MAC1, el código de identificación, el número de franqueo y dicho saldo en la tarjeta bancaria 18. Si se ha producido una fase de codificación en lugar de un cálculo MAC, las codificaciones del código de identificación, el número de franqueo y dicho saldo son almacenadas en la tarjeta bancaria.

En la fase 412, el sistema de servidor 70 manda una copia de bien el MAC1, el código de identificación, el número de franqueo y el saldo, o bien las codificaciones del código de identificación, el número de franqueo y el saldo, a la central 34. Dicha central 34 nuevamente almacena dichos datos en su memoria 40.

Después de la fase 412 se completa el almacena-

miento de un saldo en la tarjeta bancaria 18 que puede ser usado para sellos electrónicos.

La Fig. 4b muestra cómo un usuario, con su tarjeta bancaria 18 que ha sido provista de un saldo de este modo, puede dar instrucciones al PC 50 para imprimir una marca de franqueo en un artículo postal.

Una vez se haya iniciado el programa asociado, fase 450, dicho PC 50 espera hasta que el usuario haya enviado una orden de imprimir una marca de franqueo, fase 452.

Por medio de la fase 454, dicho PC 50 tiene cuáles deben ser los costes de franqueo que deben ser procesados en la marca de franqueo. El usuario puede introducir los costes de franqueo, por ejemplo, por medio del teclado 58. Es imaginable que este fase sea automatizada con la ayuda de un dispositivo de pesado automático (no mostrado), conectado a dicho PC 50, que pese el artículo postal, después de lo cual los costes de franqueo son automáticamente determinados y pasados a dicho PC 50.

El usuario ha puesto en contacto su tarjeta bancaria 18 nuevamente con el medio de entrada/salida 14 y se ha identificado nuevamente con la ayuda de su código PIN. El microprocesador 52 lee el MAC1, el código de identificación, el número de franqueo y el saldo actual de la tarjeta bancaria 18, fase 456.

El microprocesador 52 posteriormente verifica, fase 458, si el saldo actual es suficiente para los costes de franqueo deseados. Si no, sigue un mensaje al usuario luego en la fase 460, causando, por ejemplo, que el usuario deba restablecer su saldo en la tarjeta bancaria.

En la fase 462, el microprocesador 52 da instrucciones a la impresora 62 para imprimir una marca de franqueo, calculada por el SAM 64, en el artículo postal 22 después de que el usuario haya introducido el artículo postal 22 en la impresora 62. A este respecto, el SAM 64, con la tarjeta bancaria 18, calcula el MAC2 en base a todos los datos que están incluidos en la marca de franqueo, entre los que se encuentra: el código de identificación, el número de franqueo único, el saldo actual y los costes de franqueo. Como alternativa para calcular un segundo MAC, MAC2, dichos datos pueden ser codificados. Los datos preferiblemente también contienen un código de PC que únicamente identifica a dicho PC 50.

Después de la fase 462, se deduce el saldo actual en la fase 464 para substraer los costes de franqueo de éste. El nuevo saldo actual entonces representa la cantidad que aún está disponible para otros sellos electrónicos.

Cabe observar que en la forma de realización que se describe en base a las Figs. 4a, 4b y 5, se usa un número de franqueo único justo hasta que se gaste el saldo original. No obstante, puesto que el saldo actual y los costes de franqueo actuales son también incluidos en cada marca de franqueo, sigue correspondiendo una secuencia de bits única por artículo postal.

Después de la fase 464, el programa vuelve a la fase 450.

El pago por el cliente preferiblemente se produce en el momento en el que el cliente restablece el saldo en su tarjeta bancaria. Esto puede tener lugar electrónicamente de una manera conocida *per se*. A este respecto, el débito pueden producirse nuevamente, por medio de la central 34, desde el saldo de un banco central, o directamente de la tarjeta bancaria 18 si esta comprende un monedero electrónico.

Es también imaginable, no obstante, dejar que el pago se haga más tarde, como se ha explicado arriba con referencia a la forma de realización de la Fig. 1. A este respecto, el saldo cargado en la tarjeta bancaria 18 no representa una cantidad total que pueda ser gastada en sellos electrónicos, sino el número de veces que el número de franqueo provisto puede ser usado. La ventaja del pago diferido es que el usuario no necesita pesar su artículo postal 22 previamente para tener el valor de franqueo correcto incluido en la marca de franqueo 28. Después de todo, la marca de franqueo aquí también identifica únicamente al usuario, que puede recibir posteriormente la factura o cuyo saldo bancario puede ser automáticamente debitado. Además, la presencia del número de franqueo único con código de identificación y el "saldo" vigente garantiza que cada artículo postal 22 sea identificado de forma única, de modo que se pueda detectar el fraude inmediatamente.

Cabe observar asimismo que, en vez de o junto a una identificación del usuario, es posible incluir una identificación del SAM 64 en la marca de franqueo. En este caso, el propietario del PC 50 con el SAM 64 es responsable del pago correcto de los sellos postales electrónicos y del posible fraude realizado con el PC 50. Le corresponde entonces a dicho propietario someter el acceso al programa a las reglas de autorización para comprar un sello postal electrónico.

En otra forma de realización con la ayuda de un PC 50, se puede usar un PC estándar sin SAM 64. En este caso, dicho PC 50 no puede calcular de forma segura los MAC. La marca de franqueo es luego producida bien centralmente en la central 34 o en el sistema de servidor 70, y enviado a dicho PC 50. Dicho PC 50 combina entonces la marca de franqueo recibida con otras posibles Informaciones y la imprime en el artículo postal 22 con la ayuda de la impresora 62. En este caso, en lugar de trabajar con el almacenamiento de un saldo para sellos electrónicos en la tarjeta bancaria 18, se recupera una marca de franqueo cada vez de la central 34. En este caso, los pagos de sellos postales electrónicos preferiblemente se producen directamente bien debitando un saldo bancario de un usuario, o bien una tarjeta bancaria 18 con un monedero electrónico. Para luchar contra un posible fraude, el usuario debe únicamente identificarse, por ejemplo con su número de cajero automático/bancario y un PIN asociado. Preferiblemente, la identificación también se produce con la tarjeta bancaria 18 y verificando un código PIN.

Arriba se ha descrito cómo se puede generar e imprimir en un documento una marca de franqueo con una secuencia de bits única. Las reivindicaciones previstas para este proceso fueron presentadas el 20 de noviembre de 1998 con la solicitud de patente holandesa 1010616, cuya prioridad se reivindica. A continuación se explicará con mayor detalle el proceso de los documentos provistos de tal marca de franqueo, y particularmente la verificación de su validez. Como un ejemplo a este respecto, se expondrá la situación de que los documentos conciernen artículos postales. Como se ha mencionado anteriormente, los documentos no tienen que ser artículos postales.

Primero se hará una breve descripción del sistema "BriefPost 2000" (LetterMail 2000), que fue desarrollado por el PTT Post de Holanda. A ello le sigue una descripción de cómo se puede verificar la marca de franqueo en el proceso de clasificación.

BriefPost 2000

En la Fig. 6 se explica esquemáticamente la clasificación automática dentro del BriefPost 2000 y divisible en dos procesos de clasificación de "Briefpost Klein" (Correspondencia Pequeña) y "Briefpost Groot" (Correspondencia Grande), relacionados con artículos postales pequeños y grandes respectivamente.

Estas dos categorías son clasificadas por máquinas diferentes. En principio, no obstante, ambas categorías comprenden los mismos niveles de clasificación aunque implementados separadamente:

1. primer nivel de clasificación: clasifica el correo para los centros de clasificación;
2. segundo nivel de clasificación: clasifica el correo para enviar a la dirección de correo o para enviar a un apartado de correos.

En el primer nivel de clasificación, dependiente de la información en la imagen de dirección del correo, la red de ordenadores de codificación determina la información de clasificación. En principio, el sistema dispone de 30 seg. para ello - durante dicho tiempo el artículo postal está físicamente presente en la máquina de clasificación (esto no se aplica a la máquina de clasificación para el "Briefpost Groot"). La información de clasificación es posteriormente colocada en el correo en forma de índices:

1. índice de clasificación (SIX): Este índice es colocado para el "Briefpost Klein" tras la "codificación" satisfactoria; en el primer nivel de clasificación, la información de clasificación se establece con él, por ejemplo como un código de barras en el correo. En el segundo nivel de clasificación, este puede ser leído posteriormente de una forma fiable;
2. Índice de identificación (IX): Este es colocado para "Briefpost Groot", o si la codificación para "Briefpost Klein" no estaba disponible a tiempo. No se imprime un índice de clasificación (SIX), sino que se coloca un número de secuencia (IX). Cualquier información de clasificación es luego almacenada en la red de ordenadores asociada a este número. Para la máquina de clasificación para "Briefpost Groot", esto se hace para todos los artículos postales en conexión con una línea de retardo mecánica demasiado corta; para la máquina de clasificación para "Briefpost Klein", se usa este método sólo si la información de clasificación no está disponible a tiempo (dentro de 30 seg.). En el segundo nivel de clasificación, la información de clasificación es consultada en base al índice de identificación. Para "Briefpost Klein", también se puede usar un índice de identificación si el ordenador de codificación no puede determinar la información de clasificación dentro de un tiempo determinado. El correo debe luego pasar nuevamente el primer nivel de clasificación más tarde;
3. Índice de cliente (KIX): Este índice contiene, por ejemplo, el código postal y el número de casa, número de apartado postal o

número de respuesta prepagada, por ejemplo en forma de un código de barras. Este es un índice que puede ser registrado por los clientes en el correo como una parte de la dirección;

4. índice de cliente especial: Este es un índice interno usado por el PTT Post de Holanda que se fija a los artículos postales por medio de adhesivos. Dicho índice se usa, por ejemplo, para el servicio de reenvío.

Para el primer nivel de clasificación "Briefpost Klein", el proceso de codificación distingue entre codificación en línea y fuera de línea:

1. codificación en línea: Este es el proceso por el cual la información de clasificación del correo es establecida dentro de un tiempo determinado (30 seg.);
2. codificación fuera de línea: Este es el proceso por el cual, si la codificación en línea no fue satisfactoria por un exceso de tiempo, el correo es provisto de un índice de identificación (IX) y posteriormente, a partir de las imágenes de dirección almacenadas asociadas, la información de clasificación es todavía establecida, la cual, después de un segundo nivel del primer nivel de clasificación es todavía colocada en el correo.

La Fig. 7 muestra un ejemplo de una red de codificación que puede ser usada con respecto a la presente invención. La red de codificación consiste en un ordenador de codificación CC y varios medios de codificación:

1. ordenador de codificación CC (del inglés Coding Computer): Este distribuye las operaciones de codificación sobre los medios de codificación y determina la estrategia de codificación que debe llevarse a cabo por artículo postal;
2. primer lector de dirección PCD (del inglés Primary Coding Device (Dispositivo de Codificación Primario)): Este determina la información de clasificación para el grueso de todo el correo;
3. segundo lector de dirección SCD (del inglés Secondary Coding Device (Dispositivo de Codificación Secundaria)): Este intenta determinar la información de clasificación para el correo que no fue codificado por el primer lector de dirección;
4. sistema de recuperación de dirección ADB (del inglés Address Database (Base de datos de Dirección)): Este sigue intentando determinar, en el caso de resultados no fiables del primer lector de dirección PCD y del segundo lector de dirección SCD, información fiable de clasificación;
5. Estación de codificación de video VCD (del inglés Video Coding Device (Dispositivo de Codificación de Video)): Aquí la información de clasificación puede ser determinada manualmente para el correo restante;

6. unidad de descodificación DD (del inglés Decoding Device (Dispositivo de Descodificación)), que se dispone para descodificar las marcas de franqueo 28 de los artículos postales leídos.

Cabe observar que otros medios o medios alternativos de codificación son posibles en el futuro.

La red de codificación está conectada a las máquinas de clasificación. Una parte importante de la máquina de clasificación está formada por una o más Unidades de Transporte de Correo MTU (del inglés Mail Transport Unit). Cada MTU está dispuesta para leer e imprimir índices. Cada MTU está también provista de una cámara fotográfica 100 para captar imágenes del correo que sirven como datos de entrada para el ordenador de codificación.

Antes de que el correo sea procesado por una de las MTUs, este es segregado (es decir dividido en las categorías de "Briefpost Klein" y "Briefpost Groot"), colocado en recipientes (es decir cada artículo postal tiene una posición uniforme del lado de dirección y de la designación de franqueo; para ello se usa preferiblemente una marca de referencia 26 en el artículo postal) y estampado (es decir devaluación de los sellos de franqueo o valor de franqueo impreso). Esto se hace preferiblemente con la ayuda de una máquina SOSMA "Schift-, Opzet-, ene Stempelmachine" (máquina para segregar, colocar al final y estampar). La SOSMA tiene la tarea de separar ciertas corrientes del grueso del resto (por ejemplo sobres de orden de giro etc.). Para ello se aplica el código FIM.

Lector de código de barras

Hay diferentes opciones para la manera en la que se puede leer el código de barras 28 en el proceso.

Por ejemplo, se pueden utilizar las imágenes que son capturadas por las cámaras 100 en las máquinas de clasificación como datos de entrada para el proceso de codificación; a partir de dichas imágenes, por medio de una unidad de codificación especial conectada a las cámaras 100, el contenido de los códigos de barra son retrospectivamente determinados. Esto aumenta considerablemente las corrientes de datos en la red de codificación, puesto que el 100% de todas las imágenes debe ser enviadas adicionalmente a tal unidad de codificación.

Otra posibilidad es la aplicación de un lector de códigos de barras dedicado que, por ejemplo, provea una secuencia ASCII como datos de salida, que posteriormente, por medio de la red de codificación, puede ser posteriormente transportada a un sistema de base de datos de verificación. A elección, tal lector de código de barras puede ser construido en la máquina de clasificación, por ejemplo, aunque también en la SOSMA. En este caso, el impacto en el proceso de clasificación es mínimo, y los códigos de barra 28 de casi todas las corrientes de correo que deben ser manipuladas manualmente pueden ser controlados.

A veces la dirección de envío, o al menos el código postal de la misma, estará incluida en la marca de franqueo. En consecuencia, en el momento en el que la marca de franqueo es leída, también se facilita al menos una parte esencial de la dirección de envío. Esta información se puede utilizar en primer lugar para activar la lectura de la dirección de envío impresa 30 con una unidad de Reconocimiento de Caracteres Óptico (OCR), y en segundo lugar para establecer directamente si se han producido irregularidades con la

dirección de envío (y así quizás con el uso de la secuencia de bits única).

Secuencias de bits únicas y marca de franqueo

Como se ha descrito antes, la presencia de una secuencia de bits única en la marca de franqueo 28 puede ser usada como medio para indicar la validez de un franqueo (o de un documento arbitrario). El punto de partida del método es el uso de una nueva secuencia de bits única para cada transacción. Así una secuencia de bits única es, en este caso, válida sólo una vez. Tal y como se menciona, las restricciones en la capacidad de memoria de, entre otras, las tarjetas electrónicas pueden conducir a este punto de partida lo cual no era realizable (asequible) en el estado de la técnica actual (una tarjeta electrónica con la que sólo unas pocas, por ejemplo menos de 10, transacciones son posibles es muy difícil de usar de forma práctica). Se ha encontrado una solución para ello en la aplicación de un “monedero” o contador en la tarjeta electrónica en combinación con una secuencia de bits única. Tal secuencia de bits única es entonces válida para varias veces, por ejemplo en combinación con un saldo que es definido de forma precisa previamente.

Verificaciones

Las verificaciones están restringidas a aquellas que son posibles en el proceso de clasificación. Las Figs. 8 a 14 inclusive muestran flujogramas para clarificar las verificaciones.

Escaneado de la marca de franqueo (Fig. 8)

El artículo postal 22 (carta) es leído por la MTU con la cámara fotográfica 100 para establecer los datos de direcciones, fase 800. Al hacer esto, se obtiene una imagen completa de la cara frontal del artículo postal.

En esta imagen, se busca el código de barras (bidimensional) 28, fase 802. Posteriormente se analiza si el código de barras 28 contiene un sello electrónico en el sentido de la invención, fase 804. Si este no es el caso, el artículo postal es procesado como correo ordinario, fase 806.

Si un sello electrónico está presente, el código de barras 28 es interpretado/descodificado, de modo que la información se haga disponible, fase 808 (ver siguiente sección). Para ello, una unidad de descodificación especial DD (Dispositivo de Descodificación) podría ser integrada a la red de codificación (Fig. 7), además del PCD y el SCD.

Si por una razón u otra la marca de franqueo no puede ser descodificada correctamente, fase 810, el artículo postal es conducido a un proceso separado, fase 812. Posteriormente, el campo del Comprobante de pago es convalidado, fase 814. La fase 814 está aún más detallada en la Fig. 9.

Descodificación de la marca de franqueo (fase 808)

La marca de franqueo 28 contiene, por ejemplo, un código de barras 2D DataMatrix. Este contiene diferentes unidades de información, entre las que se encuentra una firma digital del remitente (persona de franqueo), información cifrada (encriptada) y datos (elementos) cifrados. La información cifrada está compuesta en sí misma por elementos de datos. Para la firma digital y el cifrado, se usa una criptografía de clave pública, la firma digital que es generada con la ayuda de la clave privada del remitente y el cifrado produciéndose con la clave pública (aplicable) del PTT Post.

Se produce un primer control en base a la firma

digital. Para controlar el pago se convalida el comprobante de pago (fase 814).

Convalidación del Comprobante de pago (fase 814)

El Comprobante de pago contiene varios elementos de elementos de datos y de control. Los elementos de control son (por ejemplo) MAC que protegen los elementos de datos (la protección puede tener lugar también por codificación o encriptación). Los elementos de datos son la marca de franqueo y las identificaciones del medio de pago (por ejemplo tarjeta electrónica 16/18), la máquina de emisión 2, 50 y la máquina de franqueo 20 (o impresora 62, si se desea), y el pago. Ver Fig. 9, donde se muestran las fases siguientes del proceso de convalidación para el uso de MAC (para el uso de codificación o encriptación, el diagrama es análogo):

1. Leer los MAC, fase 902, y controlar si los MAC leídos son válidos, fase 904. Si este no es el caso, el franqueo no es válido y se ejecuta un proceso separado, fase 906.
2. Si los MAC son válidos, leer las identificaciones de la máquina de emisión 2, 50 y la máquina de franqueo 22 (impresora 62), fase 908, y controlar sus validez, fases 908-912.
3. Leer la identificación del medio de pago y controlar si esta es la correcta. Esto puede efectuarse también en las fases 908-912 y no es un control estricto.
4. Finalmente la validez del pago debe ser verificada controlando si marca de franqueo válida (nueva, pero emitida) está impresa en el artículo postal 22, fase 914. Esto concierne a una consulta simple en la base de datos de secuencias de bits únicas en la segunda memoria 40 más el marcado de la secuencia de bits única asociada como que ha sido impresa. Si el método de “secuencia de bits única más contador”, donde el contador define bien un número de veces en las que la secuencia de bits puede ser usada o bien se usa un saldo, se aplica lo siguiente: la combinación de secuencia de bits única y contador debe ser controlada. Como se ha observado antes, la combinación de secuencia de bits, aunque se use más de una vez, y el contador sigue siendo única para cada franqueo. En primer lugar, con la ayuda de la base de datos 40 se puede determinar la validez de la secuencia de bits única. Después de todo, ésta debe haber sido emitida. También se puede controlar si la secuencia de bits ha recibido un cierto periodo de validez. En función de la forma de pago (antes de proveer la secuencia de bits única o después de procesar un artículo postal asociado por la oficina postal), se debe registrar qué ha sido provisto y/o impreso. En el caso de que no se haya provisto secuencias de bits únicas, ya impresas antes, y/o que ya no sean válidas, el franqueo no es válido.

Si hay mención de una secuencia de bits única, para la que un cierto saldo está asociado, la combinación de dicha secuencia de bits y dicho saldo (valor

de contador) deberá estar presente en la memoria 40. Específicamente debe ser evidente que tal combinación no fue impresa en un artículo postal antes. Posteriormente, esta combinación debe ser designada como habiendo sido impresa y ya no es válida.

En la base de datos 40, se pueden almacenar los datos siguientes para cada secuencia de bits única:

1. la fecha de emisión y periodo de validez,
2. la forma de pago permitida (antes de su provisión o después de la impresión en un artículo postal) y
3. las combinaciones de la secuencia de bits con el saldo (valores de contador) impresos en los artículos postales. Nota: también es posible mantener sólo un valor de contador vigente centralmente y, tras detectar una secuencia de bits con un cierto valor de contador, modificar este valor de contador registrado centralmente. Esto se explicará a continuación.

El procesamiento y la verificación en base a esto se explica en base a las fases 1002-1014 en el flujo-grama de la Fig. 10, que habla por sí mismo.

Dependiendo de la forma de pago, prepago o pago diferido, se registra el uso de forma diferente. También son posibles implementaciones más simples y más fundamentales de las verificaciones como se explicará a continuación.

Pago por anticipado (prepago)

En principio, un grupo de secuencias de bits únicas determinado está presente en la tarjeta 18, cuya secuencias de bits son marcadas como tales en la base de datos 40 cuando se vende la tarjeta 18. Las secuencias de bits únicas pueden cada una representar un determinado valor (fijo) o cada una ser usada en combinación con un contador (saldo). En cada caso se mantiene que: después de usar el(los) contador(es), las secuencias de bits únicas son inválidas.

Para las secuencias de bits pagadas por anticipo, se registra el saldo inicial (por secuencia de bits única o totalmente por tarjeta 18, es decir, por grupo de secuencias de bits únicas). Para cada franqueo, una parte de este saldo es entonces sustraída. Cuando se gasta el saldo se gasta la secuencia de bits.

El proceso de control es el mismo que aquél para las tarjetas recargables "normales".

En primera instancia se puede implementar el método simple, Fig. 11, hasta que haya una razón suficiente para implementar el más fundamental, Fig. 12.

Simple

En el caso más simple, tal como se ha explicado en base a las fases 1102-1108 de la Fig. 11, sólo se mantiene un valor total. Aquí no es posible, por ejemplo, detectar copias hasta que el valor de contador registrado en el valor de contador registrado centralmente (memoria 40) se haga cero. Se tiene sin embargo la garantía de que en última instancia se descubrirá un uso abusivo y que el uso abusivo no podrá ser superior al saldo inicial.

Fundamental

Si todos los franqueos están registrados, es decir para las secuencias de bits únicas se registra qué valores de contador han sido realmente impresos en un artículo postal, entonces se pueden detectar las copias. Los valores de contador individuales deben reflejar que el valor de contador inicial ha sido gastado

consecutivamente. Esto se explica con mayor detalle en base a las fases 1202-1208 en el flujograma de la Fig. 12.

El valor de contador inicial puede ser considerado como un intervalo. Cada valor de contador es un subintervalo del mismo. Ahora la intersección de cada par de subintervalos debe ser vaciada y la unión de todos los subintervalos debe cubrir el valor de contador inicial. Esto último no tiene que producirse como un total, por ejemplo porque ciertos artículos postales franqueados nunca fueron ofrecidos para el envío, o porque no se ha usado una parte del saldo.

Pago retrospectivo (pago diferido)

Aquí también se aplican dos métodos. En principio, se "gasta" una secuencia de bits única para cada transacción.

Por cuestiones de implementación técnica, se puede elegir entre el uso de una secuencia de bits única para una serie de transacciones que debe ser definida. Además del "gasto" de la secuencia de bits, se aplica también un contador para el franqueo que, al igual que en las máquinas de franqueo convencionales, registra el uso que debe ser cargado.

Se puede imponer un límite en el saldo que puede ser usado (por tiempo o dinero). Una vez excedido éste, se requiere la recarga de la tarjeta 18.

Para el pago diferido, por ejemplo, se incrementa en uno un contador, o por el valor franqueado, para cada franqueo. Esto es posible hasta que se alcance un cierto límite, después de lo cual se requiere la recarga previamente mencionada de la tarjeta. En el momento de recargar, el soporte de la tarjeta puede ser "descargado" por el consumo hasta ese momento, evidentemente siempre que se pueda garantizar el pago del objeto franqueado.

Una variante de implementación consiste en deducir realmente el contador de un valor máximo, que puede ser simplemente configurado con la compra. Tan pronto como el contador alcanza 0, la secuencia de bits se invalida. Para el uso ilimitado, el límite puede ser configurado hacia un valor extremadamente grande que sea suficiente por motivos prácticos.

Simple

Si el control de duplicados no es tenido en cuenta, entonces, en primera instancia, bastará mantener el número de franqueos: véase las fases 1302-1308 de la Fig. 13. La opción de saldo usado no está indicada en la figura, pero trabaja análogamente.

Fundamental

Para controlar duplicados, todos los valores de contador individuales para la secuencia de bits única deben ser mantenidos. En principio, un mapa de bits, por ejemplo, es el medio apropiado para ello. Esto se explica con mayor detalle en base a las fases 1402-1408 de la Fig. 14. Dado que los valores de contador son, en principio, consecutivos, y los artículos postales una vez franqueados debe ser ofrecidos dentro de un periodo limitado, el tamaño real del mapa de bits puede ser restringido para mantener qué valor de contador fue el último antes del inicio del periodo asociado. Este estado y el mapa de bits son modificados diariamente. Aquí tampoco se incluye en la figura la opción de utilizar un saldo usado.

Híbrido

En primera instancia, el método híbrido es idéntico al del prepago. El control y el registro del uso asociado a éste es en consecuencia idéntico.

Sólo después de que se active la posibilidad de pa-

go diferido, el control y el registro asociados a éste serán tenidos en cuenta. Puesto que en general sólo un número limitado de franqueos será aquí pertinente, se puede usar un mapa de bits para medir.

En primera instancia, se gastará el prepago, después de lo cual se usará el contador. Tan pronto como el contador esté a 0 (o haya alcanzado su límite máximo), la secuencia de bits única se gasta.

Otros aspectos: uso óptimo de recursos de ordenador y tiempo de unidad central de procesamiento.

Tal y como se menciona, un artículo postal es mantenido dentro de la máquina de clasificación durante un cierto periodo de tiempo máximo (30 segundos) en "Briefpost Klein", durante el primer nivel de clasificación de BriefPost 2000, para obtener la información de clasificación (código postal). Si está presente, el código postal puede ser obtenido de la marca de franqueo 28 rápidamente y de una forma fiable (durante dichos 30 segundos).

En Holanda la situación es tal que, después del nivel de clasificación, los artículos postales son llevados al centro de clasificación del destino, donde tiene lugar un segundo nivel de clasificación, ver también Fig. 6. Hay un tiempo, en particular tiempo de ordenador, entre el primer y segundo nivel de clasificación, que es más largo en proporción a la demora entre el primer y el segundo nivel de clasificación (a veces el segundo nivel de clasificación tiene lugar en otro centro). Este tiempo puede ser usado como tiempo de ordenador para llevar a cabo las verificaciones necesarias.

Las secuencias de bits únicas detectadas en el primer nivel de clasificación (posiblemente con valor de contador) pueden ser colocadas en un soporte de datos físicos (CDROM) para la distribución física posterior, con los artículos postales. Obviamente se puede realizar la transferencia de dicho datos por una conexión en red.

Durante el segundo nivel de clasificación puede tener lugar un control casi completo, puesto que luego la base de datos original (central) está disponible, junto con todas las secuencias de bits únicas detectadas

en aquel día (+ valores de contador). De esta manera se superan los problemas de separación geográfica de los centros de clasificación.

Antes de ser transportadas a un centro de control, las secuencias de bits únicas leídas durante el primer nivel de clasificación pueden ser dispuestas en una secuencia de la forma lo más ventajosa posible para el control, de modo que durante el control real se requiera el menor tiempo posible. Tal una secuencia ventajosa puede ser (alfa)numérica, por ejemplo.

El control puede producirse físicamente en la central 34. En lugar de ello, no obstante, el control también se puede producir en un número de centros geográficamente separados, por ejemplo en aquellos centros donde tiene lugar el segundo nivel de clasificación. Esto hace más difícil mantener una base de datos central en la central 34, pues requiere el transporte de secuencias de bits únicas emitidas al centro de control separado por medio de un soporte de datos o por medio de una conexión en red adecuada entre el centro de control y la central 34. Debe observarse que los duplicados (ilegales) de marcas de franqueo en los artículos postales ofrecidos a los distintos centros de clasificación pueden ser identificados en el segundo nivel de clasificación.

En el caso de que la dirección de envío esté incluida en la marca de franqueo de una manera protegida, ya no es posible copiar la marca de franqueo de una manera simple para enviar el correo a las distintas direcciones de envío (destinatarios).

Además, resultará evidente al experto que, aunque todos los procesadores y SAM descritos hasta aquí han sido mostrados como bloques únicos, estos pueden ser implementados en la práctica de cualquier otra manera conocida, es decir, como, por ejemplo, diferentes subprocesadores que cooperan entre sí que, a elección, estén situados a cierta distancia el uno del otro y proporcionen la funcionalidad deseada. Estos son preferiblemente controlados por un software pero, cuando sea necesario, pueden comprender circuitos analógicos y digitales.

REIVINDICACIONES

1. Método para producir y verificar marcas de franqueo (28), que comprende las fases consecutivas de:

- a) almacenar un grupo de secuencias de bits únicas en una primera memoria (38) en una oficina central (34), conectada a una pluralidad de terminales (2);
- b) proporcionar una o más de dichas secuencias de bits únicas a por lo menos uno de dichos terminales (2);
- c) recibir de al menos uno de dicho terminales (2) una copia de las secuencias de bits únicas emitidas en combinación con un código de identificación y almacenar dicha copia de dichas secuencias de bits únicas emitidas en combinación con dicho código de identificación en una segunda memoria (40) en la oficina central;
- d) leer (800-804) una marca de franqueo (28) después de que ésta haya sido impresa en un documento, dicha marca de franqueo comprendiendo un código de identificación codificado y una secuencia de bits única codificada;
- e) descodificar (808-810) la marca de franqueo (28) para hacer un código de identificación descodificada y una secuencia de bits única descodificada;
- f) controlar (908-910) si el código de identificación descodificado es correcto comparándolo con los datos almacenados en la segunda memoria (40); y
- g) controlar (1002-1014) si la secuencia de bits única descodificada es válida comparándola con los datos almacenados en la segunda memoria (40).

2. Método según la reivindicación 1, donde el código de identificación y la secuencia de bits única están protegidos con la ayuda de un Código de Autenticación de Mensaje o, alternativamente, mediante codificación, el método comprendiendo también la fase de controlar (902-904) el Código de Autenticación de Mensaje o la codificación.

3. Método según la reivindicación 1 o 2, donde la marca de franqueo comprende un código de identificación de terminal en relación con un terminal que proveyó la secuencia de bits única a un usuario.

4. Método según cualquiera de las reivindicaciones precedentes, donde el código de identificación comprende un código de identificación de usuario y/o un código de identificación de impresión, dicho código de identificación de impresión estando asociado a un dispositivo de impresión que imprimió la marca de franqueo.

5. Método según cualquiera de las reivindicaciones precedentes, donde la marca de franqueo comprende una combinación de la secuencia de bits única y un valor de contador, el método comprendiendo también las fases siguientes:

- h. substraer el valor de contador de un valor de contador restante almacenado con dicha

secuencia de bits única en dicha memoria (40) y controlar si las cantidades de valor de contador restantes son superior a cero, y, si es así, establecer entonces que la marca de franqueo es válida, y, si no, establecer entonces que la marca de franqueo es inválida.

6. Método según cualquiera de las reivindicaciones 1 a 4 inclusive, donde la marca de franqueo comprende una combinación de la secuencia de bits única y un valor de contador, el método comprendiendo también las fases siguientes:

- i. controlar si dicha combinación ocurre en dicha memoria (40), y, si es así, establecer entonces que la marca de franqueo es válida, y, si no, establecer entonces que la marca de franqueo es inválida.

7. Método según cualquiera de las reivindicaciones anteriores, donde también se verifica si ha expirado un periodo de validez asociado a la marca de franqueo.

8. Método según la reivindicación 5, 6 o 7, donde, si se ha establecido que la marca de franqueo es válida, se inicia una rutina para el pago diferido automático de una cuenta asociada a la marca de franqueo.

9. Método según cualquiera de las reivindicaciones anteriores, donde la marca de franqueo es colocada en un artículo postal que, por necesidades de envío es clasificado en al menos un primer y luego en un segundo centro de clasificación, y en el cual las fases d y e son ejecutadas en el primer centro de clasificación y la información obtenida de ahí es enviada a un centro de control, después de lo cual las fases f y g son ejecutadas en el centro de control antes de la clasificación en el segundo centro de clasificación.

10. Sistema para producir y verificar una marca de franqueo (28) que comprende medios para:

- a) almacenar un grupo de secuencias de bits únicas en una primera memoria (38) en una oficina central (34), conectada a una pluralidad de terminales (2);
- b) proporcionar una o más de dichas secuencias de bits únicas a por lo menos uno de dicho terminales (2);
- c) recibir de al menos uno de dicho terminales (2) una copia de las secuencias de bits únicas emitidas en combinación con un código de identificación y almacenar dicha copia de dichas secuencias de bits únicas emitidas en combinación con dicho código de identificación en una segunda memoria (40) en la oficina central;
- d) leer (800-804) una marca de franqueo (28) después de que haya sido impresa en un documento, dicha marca de franqueo comprendiendo un código de identificación codificado y una secuencia de bits única codificada;
- e) descodificar (808-810) la marca de franqueo (28) para hacer un código de identificación descodificado y una secuencia de bits única descodificada;
- f) controlar (908-910) si el código de identi-

ficación descodificado es correcto comparándolo con los datos almacenados en la segunda memoria (40); y

- g) controlar (1002-1014) si la secuencia de bits única descodificada es válida comparándola con los datos almacenados en la segunda memoria (40).

11. Sistema según la reivindicación 10, donde el código de identificación y la secuencia de bits única están protegidos con la ayuda de un Código de Autenticación de Mensaje o, de forma alternativa, mediante codificación, el sistema comprendiendo también la fase de controlar (902-904) el Código de Autenticación de Mensaje o la codificación.

12. Sistema según la reivindicación 10 u 11, donde la marca de franqueo comprende un código de identificación de terminal en relación con un terminal que proveyó la secuencia de bits única a un usuario.

13. Sistema según cualquiera de las reivindicaciones 10 a 12 inclusive, donde el código de identificación comprende un código de identificación de usuario y/o un código de identificación de impresión, dicho código de identificación de impresión estando asociado a un dispositivo de impresión que imprimió la marca de franqueo.

14. Sistema según cualquiera de las reivindicaciones 10 a 13 inclusive, donde la marca de franqueo comprende una combinación de la secuencia de bits única y un valor de contador, el sistema comprendiendo también medios para:

- h. sustraer del valor de contador un valor de contador restante almacenado con dicha secuencia de bits única en dicha memoria (40), y controlar si las cantidades de valor

de contador restante es superior a cero, y, si es así, establecer entonces que la marca de franqueo es válida, y, si no, establecer entonces que la marca de franqueo es inválida.

15. Sistema según cualquiera de las reivindicaciones 10 a 14 inclusive, donde la marca de franqueo comprende una combinación de la secuencia de bits única y un valor de contador, el sistema comprendiendo también medios para:

- i. controlar si dicha combinación ocurre en dicha memoria (40), y, si es así, establecer entonces que la marca de franqueo es válida, y, si no, establecer entonces que la marca de franqueo es inválida.

16. Sistema según cualquiera de las reivindicaciones 10 a 15 inclusive, también provisto de medios para controlar si ha expirado un periodo de validez asociado a la marca de franqueo.

17. Sistema según la reivindicación 14, 15, o 16, que, si se ha establecido que la marca de franqueo es válida, inicia una rutina para el pago diferido automático de una cuenta asociada a la marca de franqueo.

18. Sistema según cualquiera de las reivindicaciones 10 a 17 inclusive, donde la marca de franqueo es colocada en un artículo postal que, por necesidades de envío es clasificado en al menos un primer y luego un segundo centro de clasificación, y en el cual el sistema en el primer centro de clasificación comprende medios dispuestos para ejecutar las fases d y e y para enviar la información obtenida de dichas fases d y e a un centro de control, el centro de control comprendiendo medios para ejecutar las fases f y g antes de la clasificación en el segundo centro de clasificación.

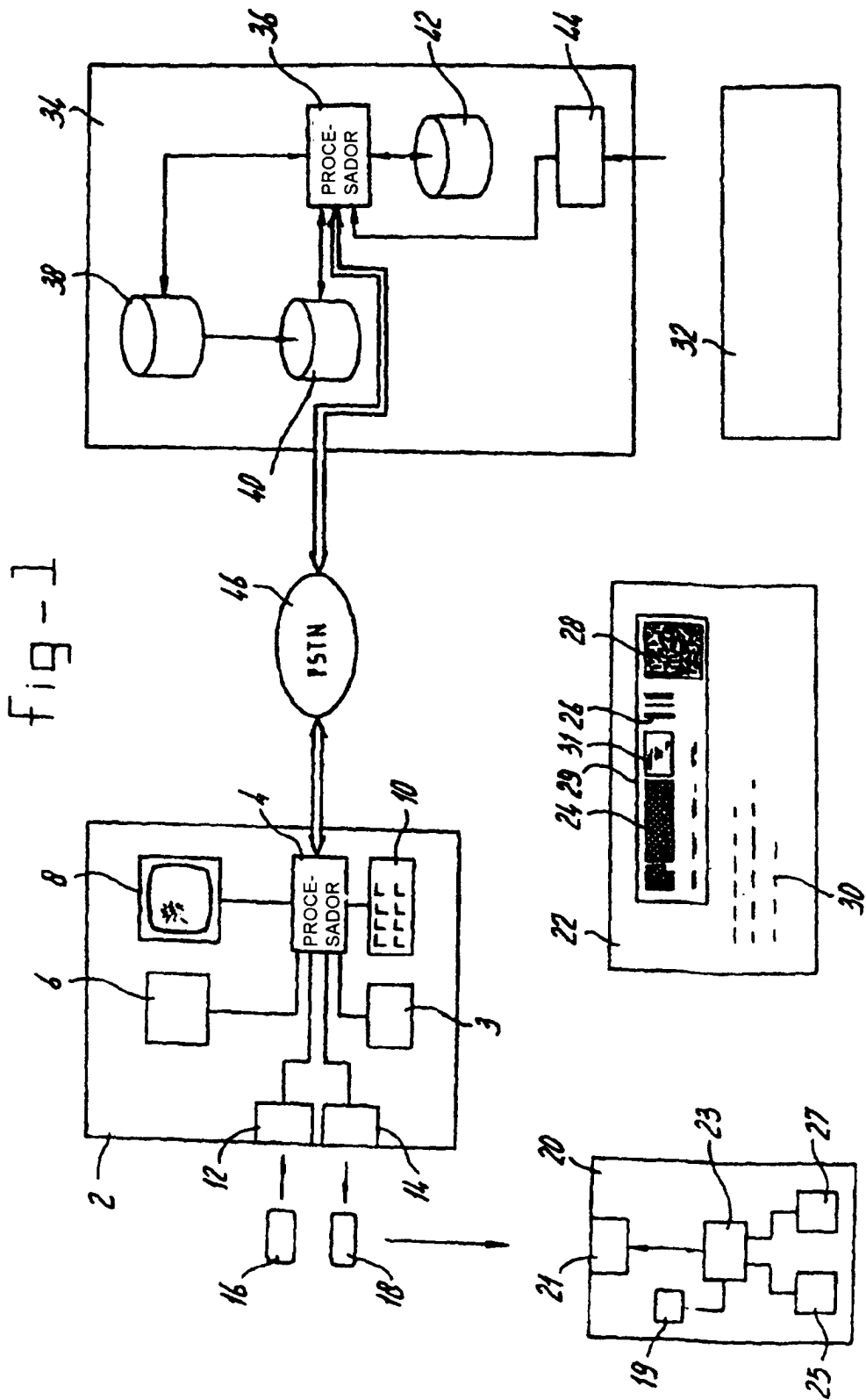
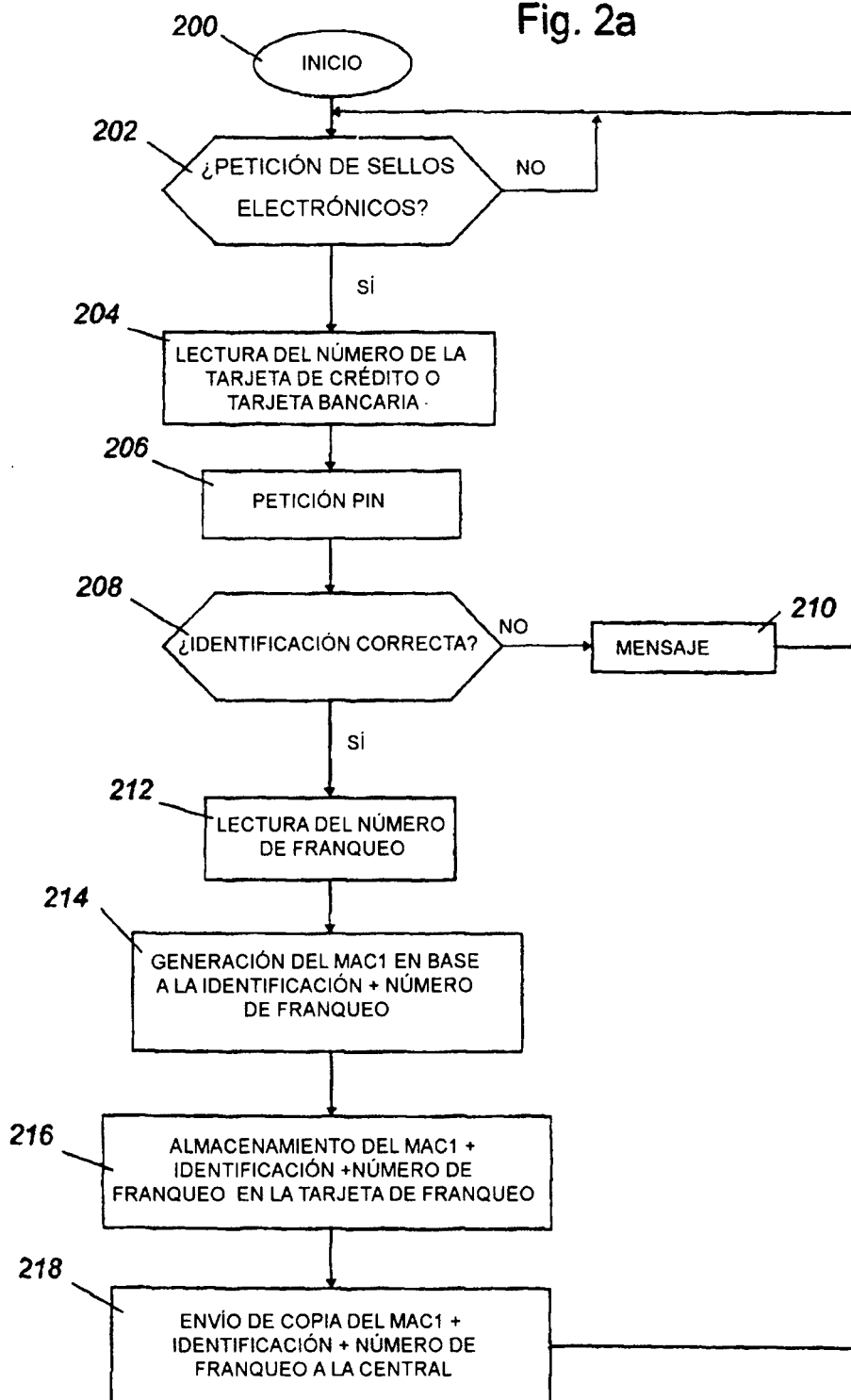
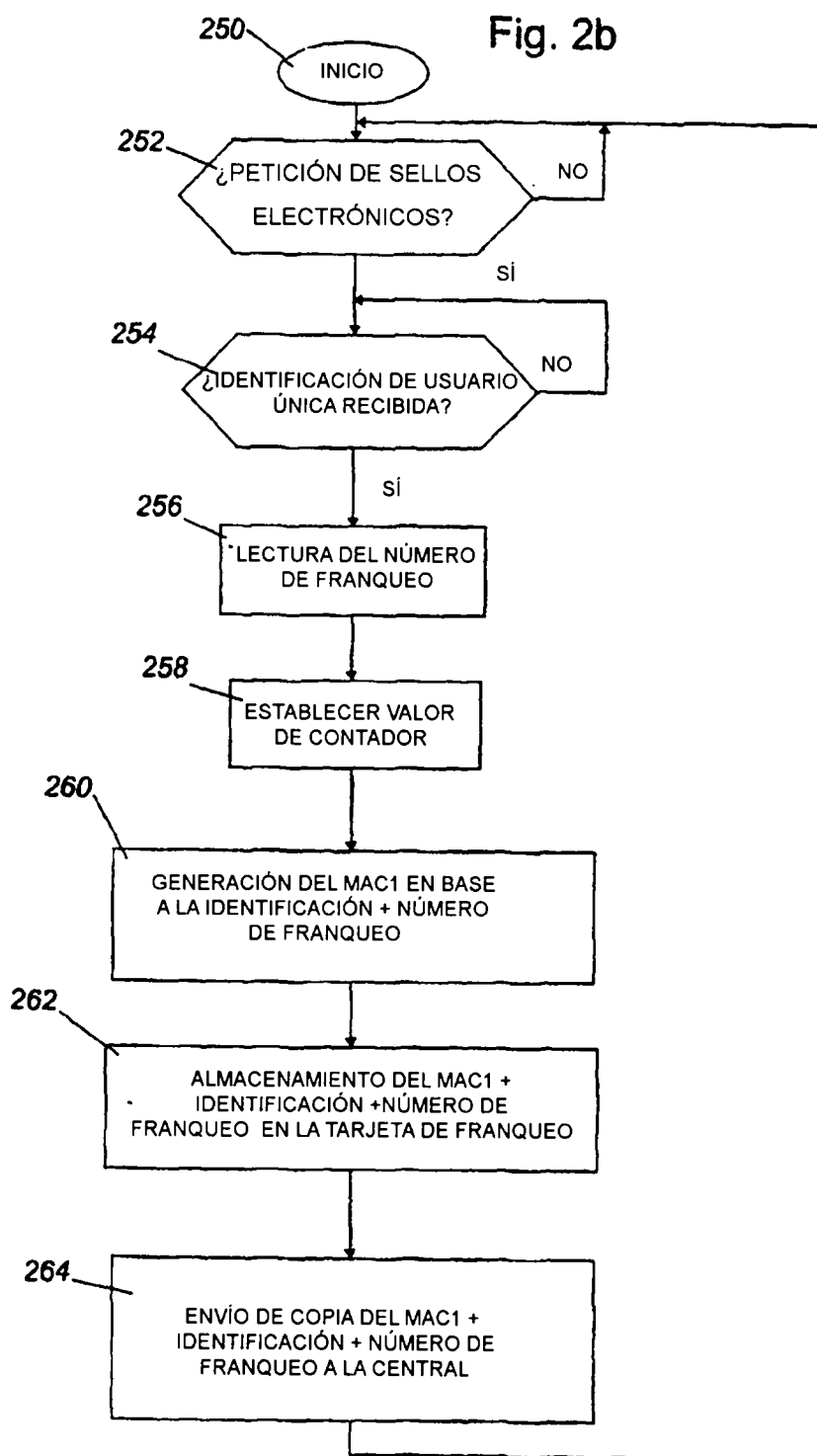


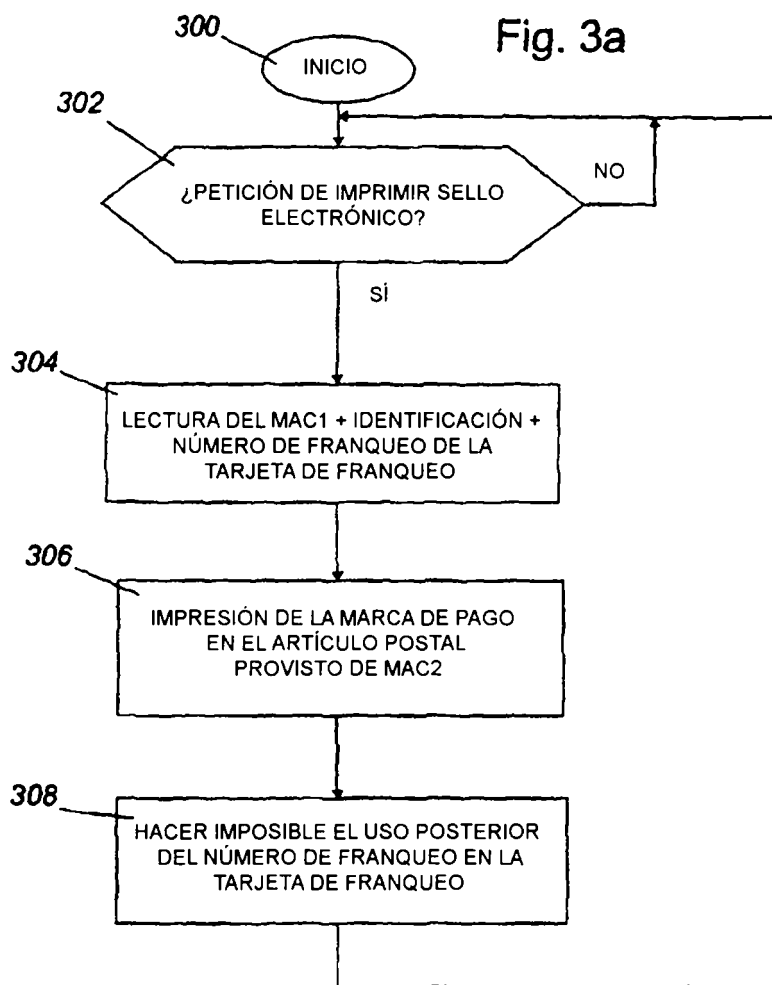
Fig. 2a



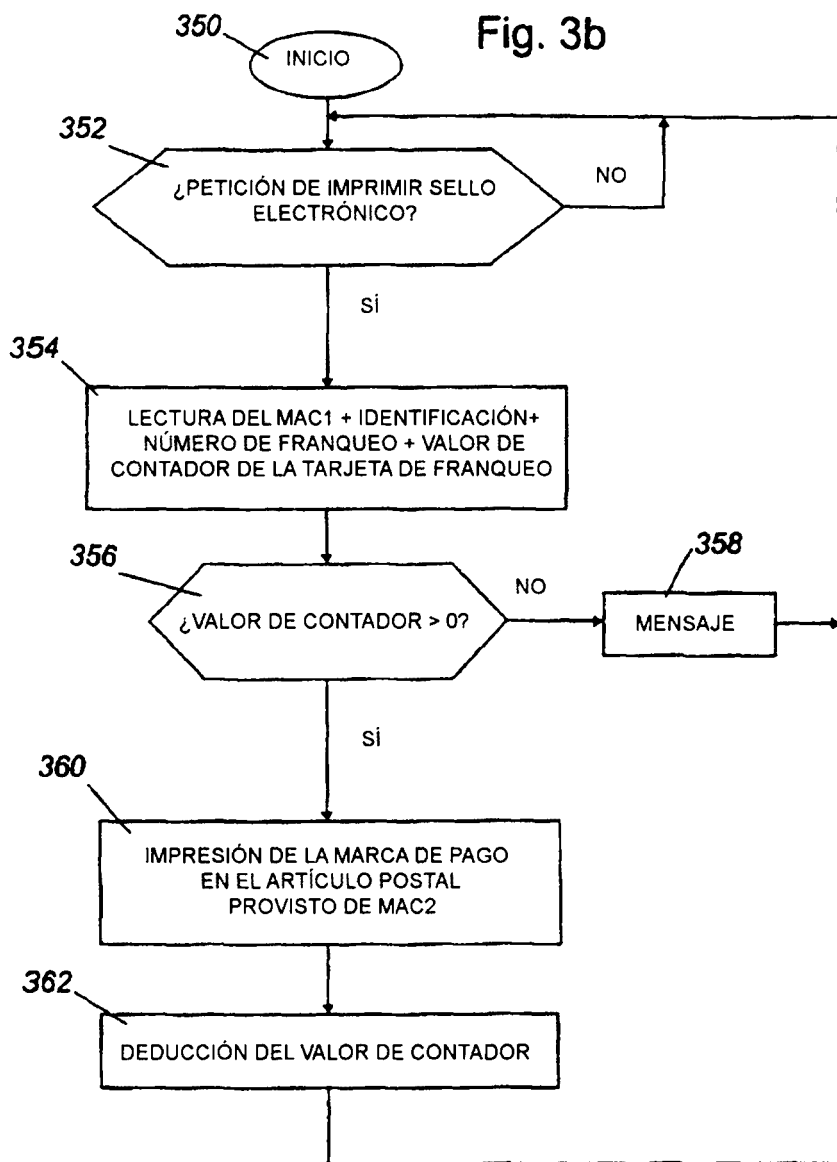
EMISIÓN DE SELLO ELECTRÓNICO



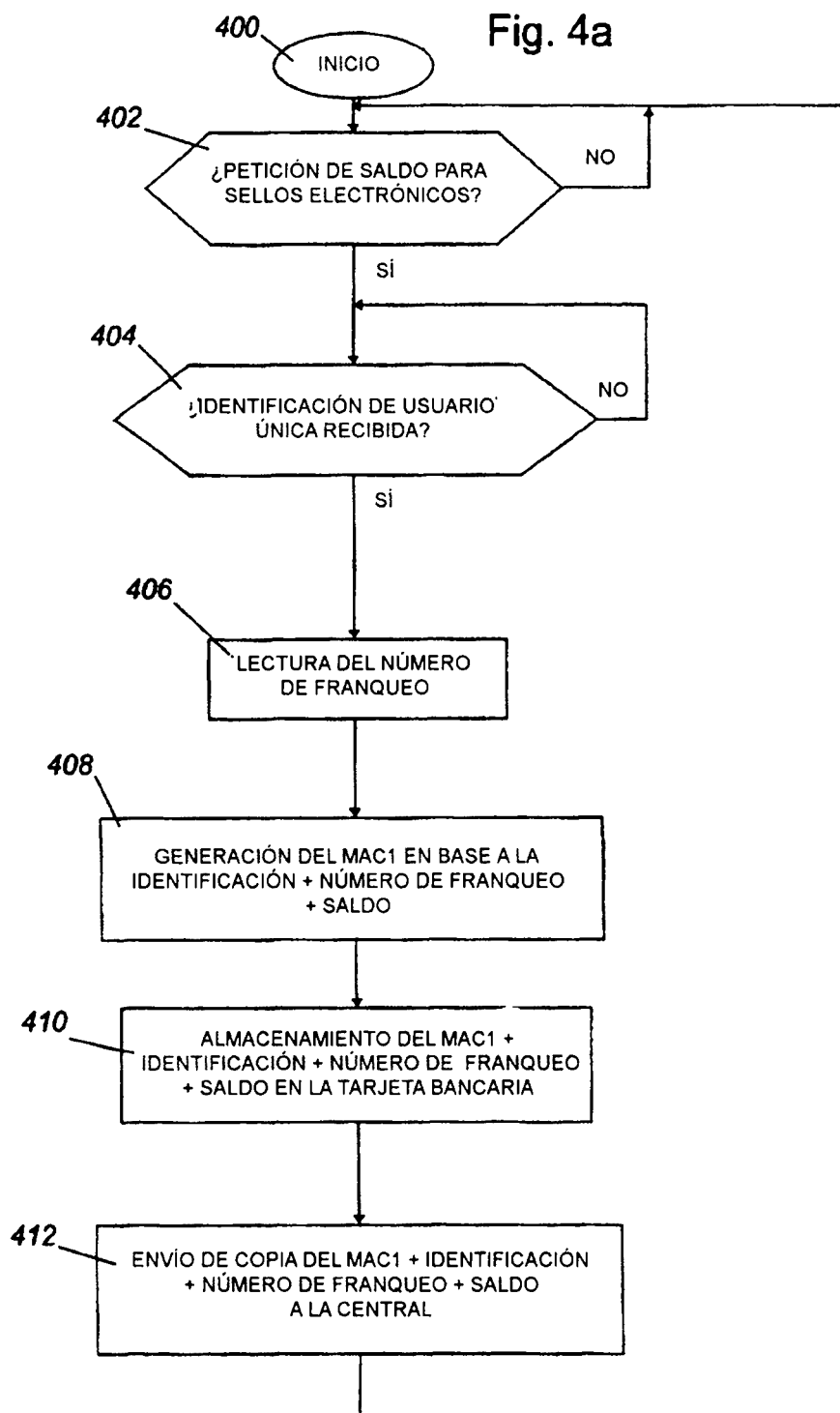
EMISIÓN DE SELLO ELECTRÓNICO CON CONTADOR



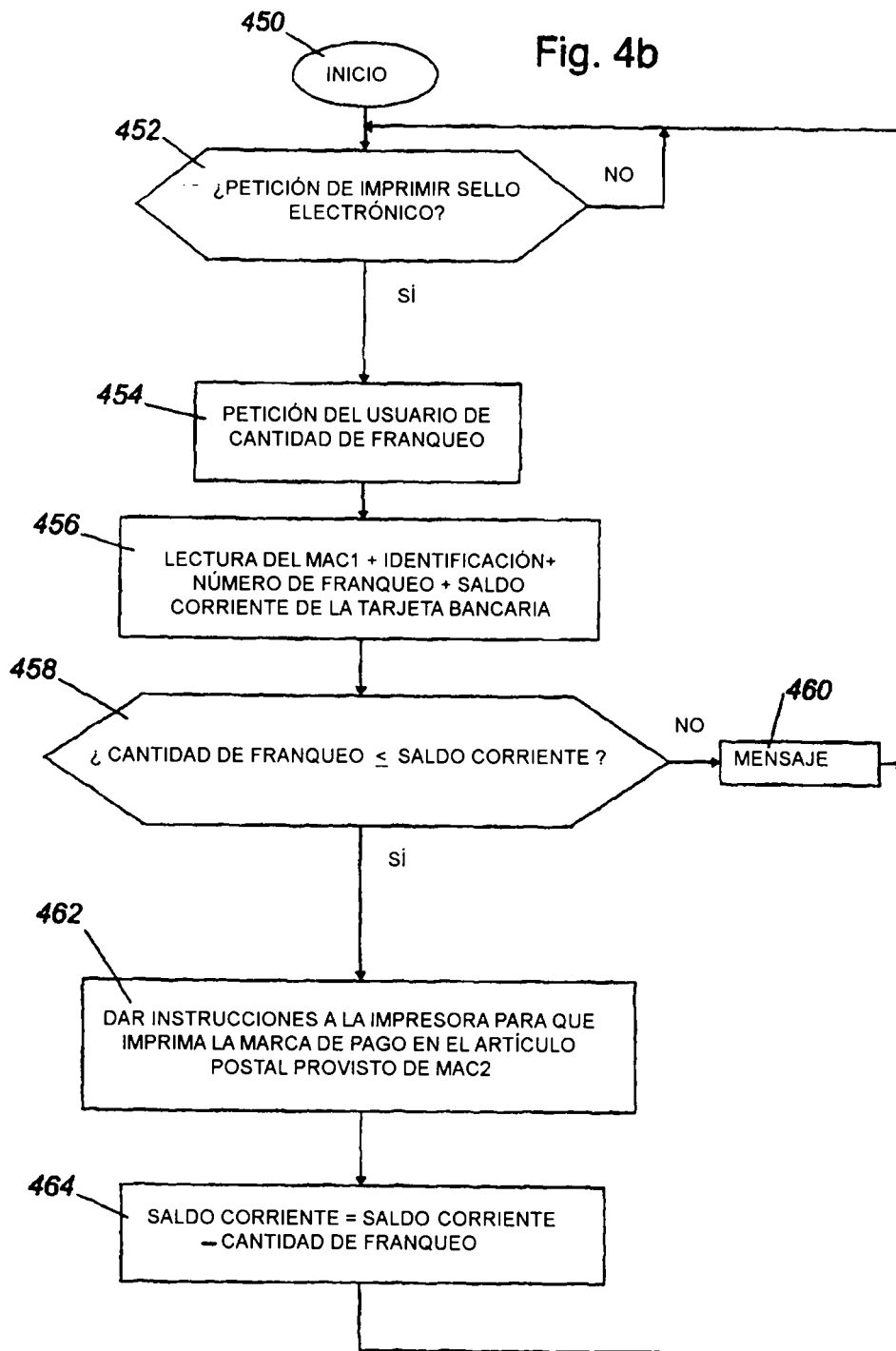
IMPRESIÓN DE SELLO ELECTRÓNICO



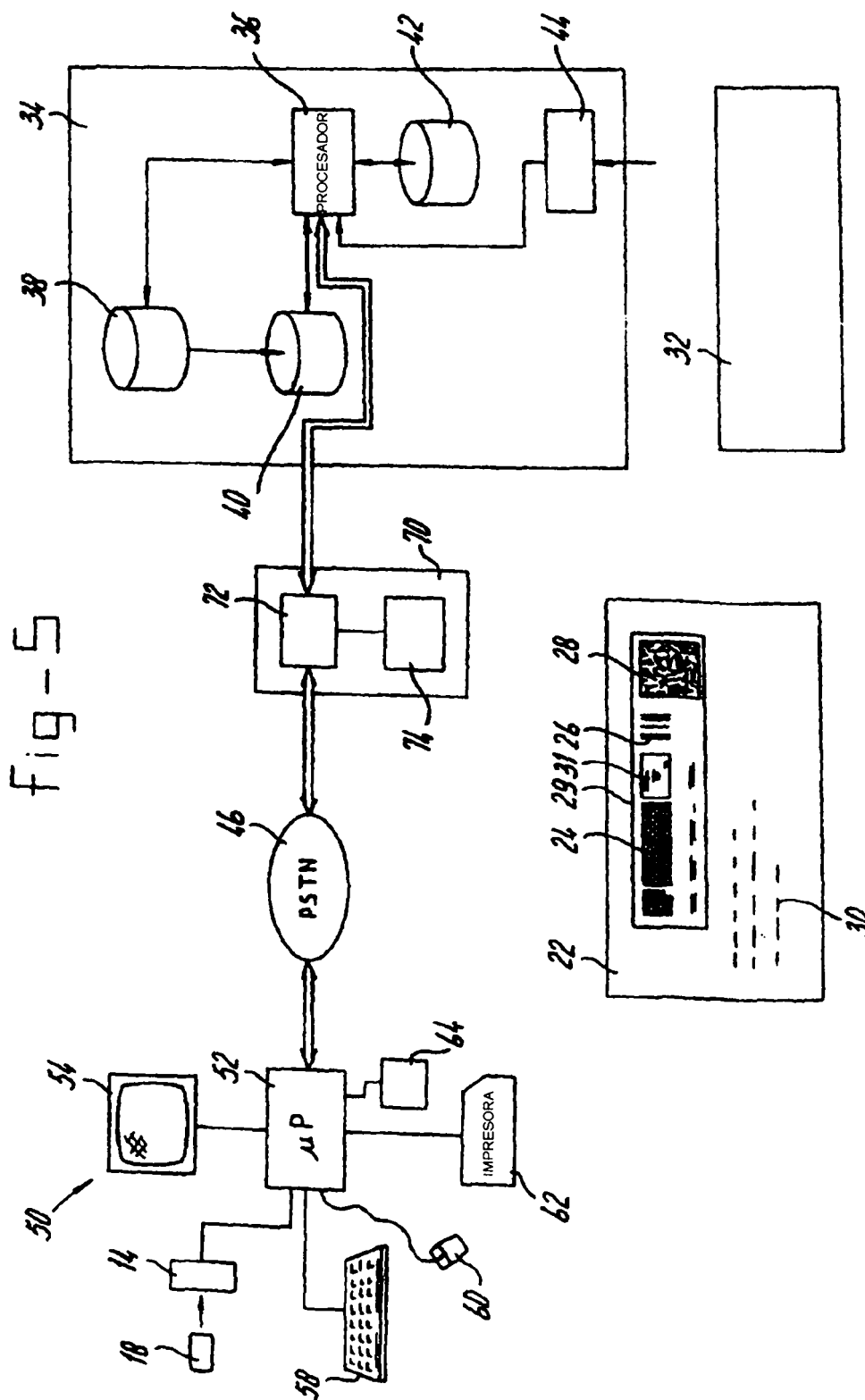
IMPRESIÓN CON CONTADOR



ALMACENAMIENTO DE SELLO ELECTRÓNICO EN LA FORMA DE REALIZACIÓN CON PC



IMPRESIÓN A TRAVÉS DE LA FORMA DE REALIZACIÓN CON PC



CATEGORIZACIÓN DE LOS PROCESOS EN UN DÍA DE CLASIFICACIÓN

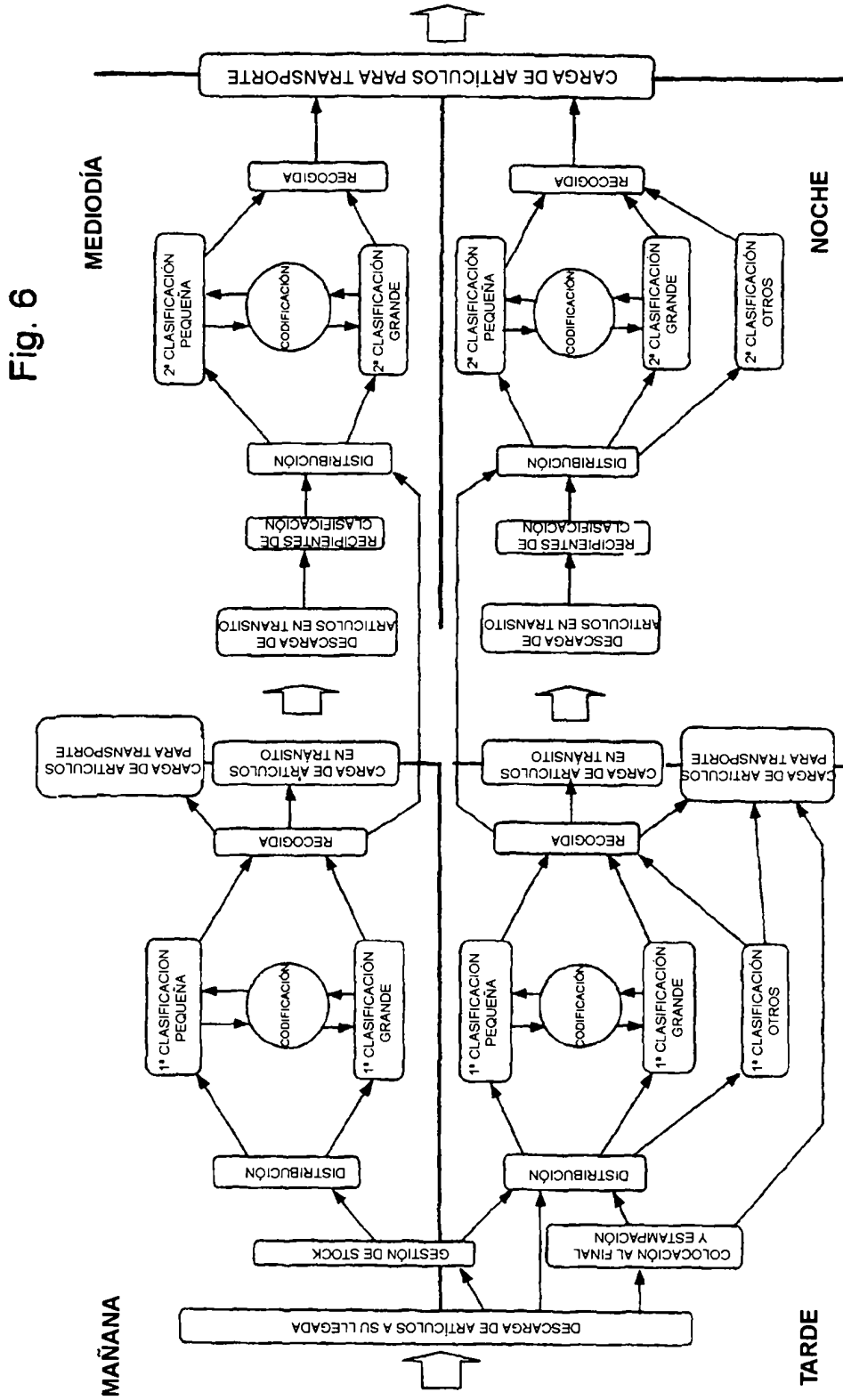


Fig. 7

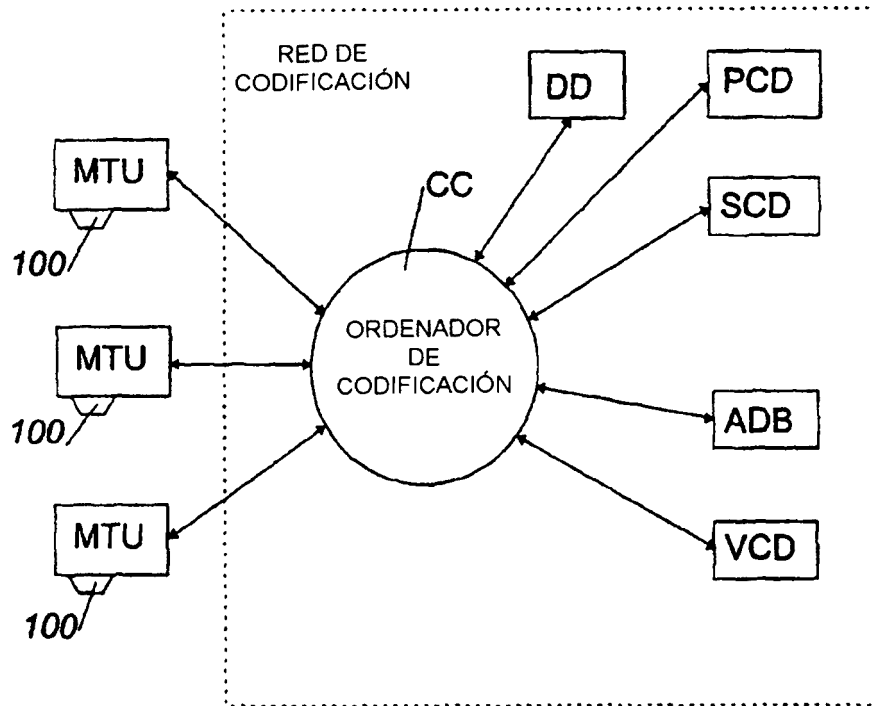


Fig. 8

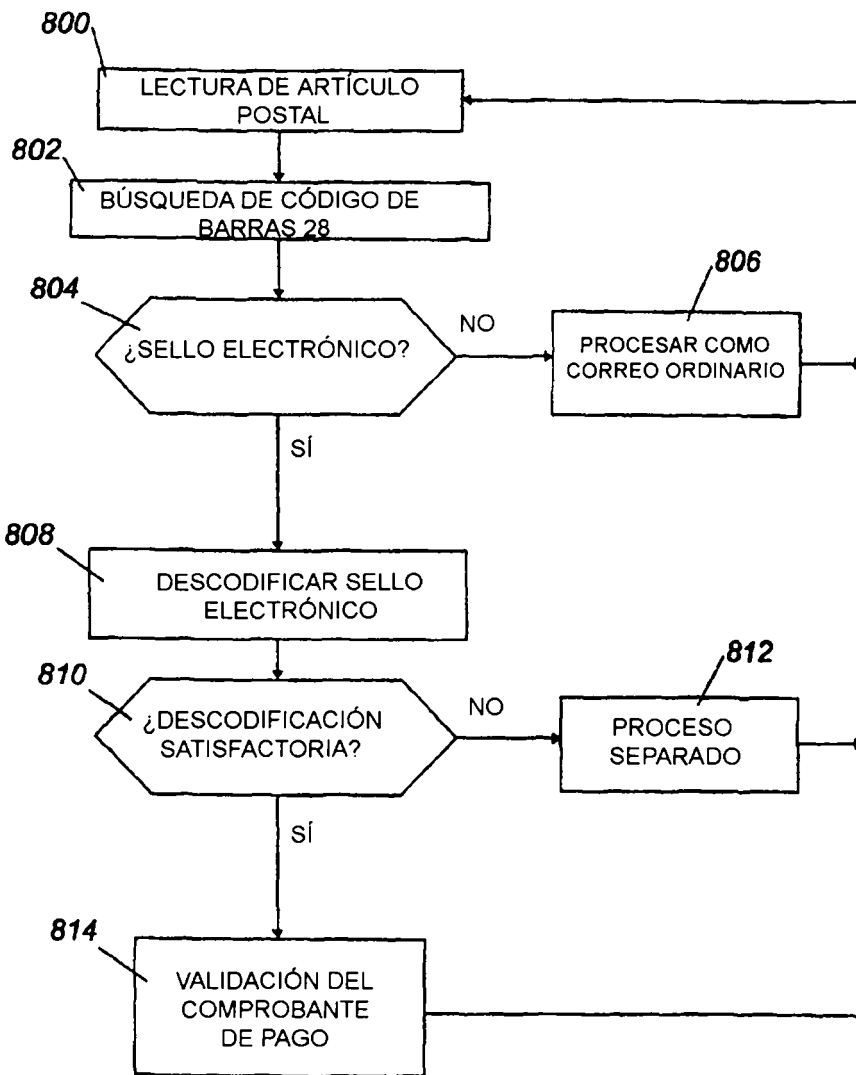


Fig. 9

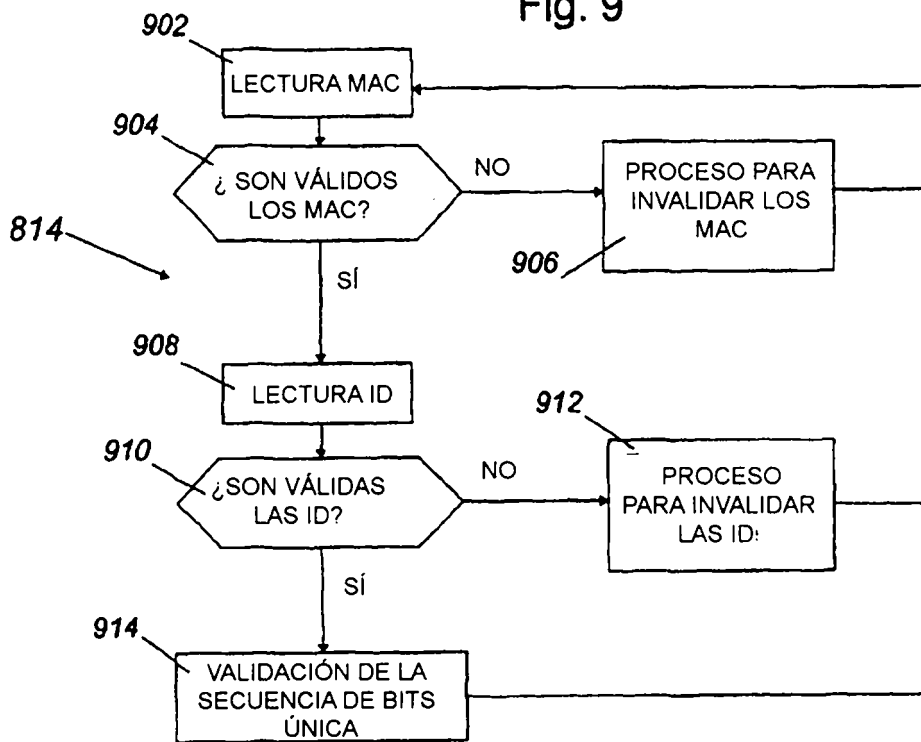


Fig. 10

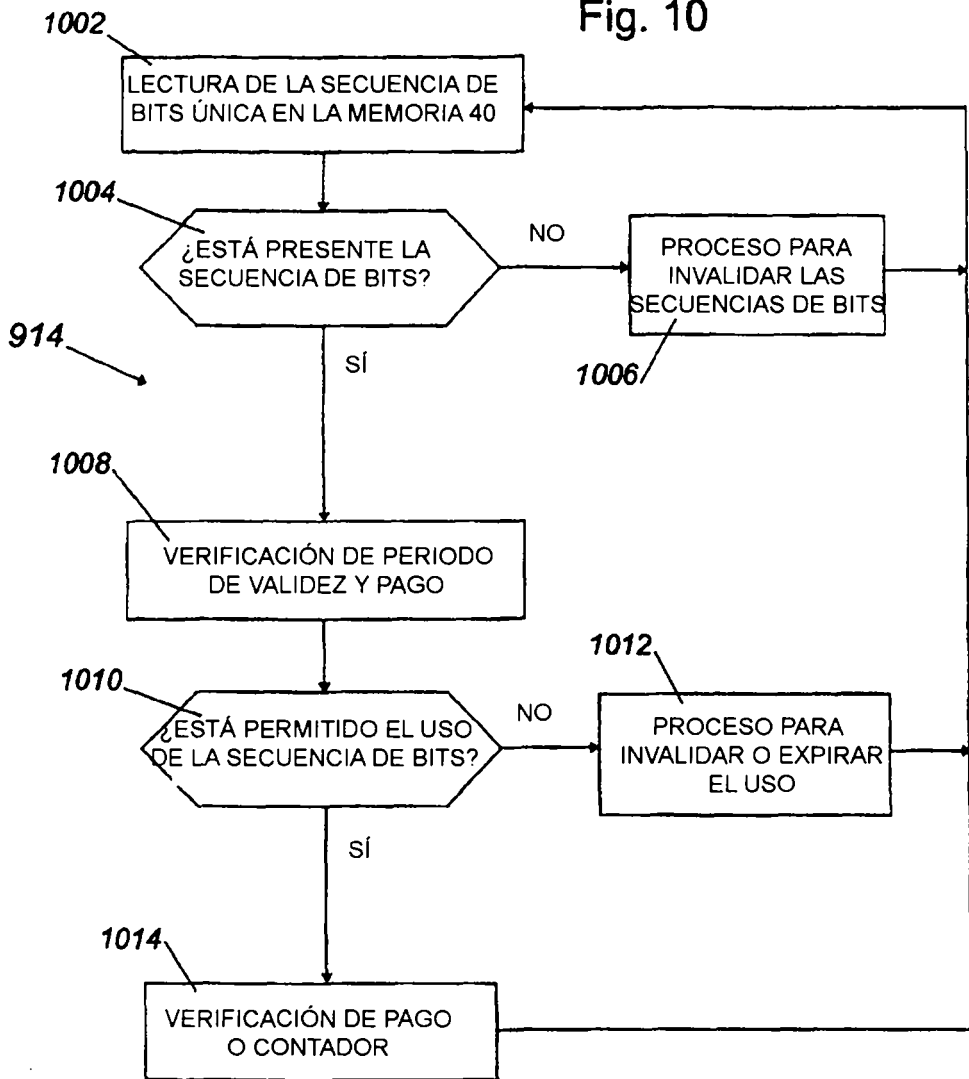


Fig. 11

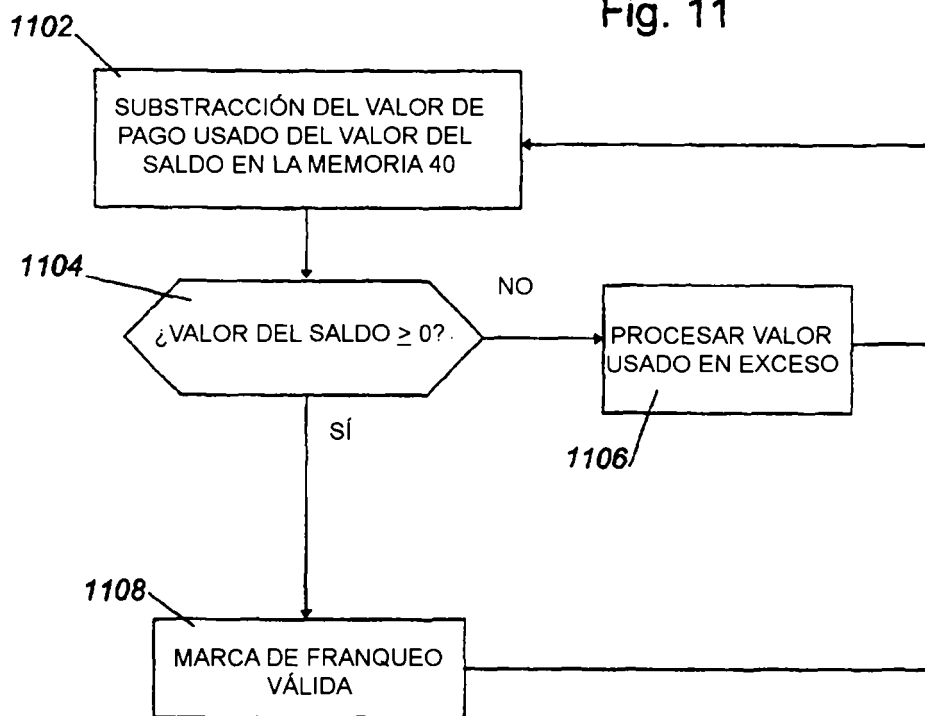


Fig. 12

