(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 440 250**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/22 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.09.2007 E 07820143 (1)**

(97) Fecha y número de publicación de la concesión europea: **06.11.2013 EP 2067341**

(54) Título: **Sistema informático y método de firma, verificación de firma y/o archivo**

(30) Prioridad:

12.09.2006 DE 102006043497

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.01.2014

(73) Titular/es:

BUNDESDRUCKEREI GMBH (100.0%)
ORANIENSTRASSE 91
10958 BERLIN, DE

(72) Inventor/es:

ZISKA, ANDREAS

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Sistema informático y método de firma, verificación de firma y/o archivo.

La invención se refiere a un sistema informático, así como a un procedimiento, para la firma, verificación de firma y/o archivo de datos y a un producto de programa informático correspondiente.

Los procedimientos para la firma electrónica de documentos son conocidos en sí por el estado de la técnica. Para la firma electrónica de un documento se genera un par de claves que está formado por una clave secreta (la llamada “clave privada”) y una clave conocida (llamada “clave pública”). En general a partir del documento es generado un valor HASH con una función HASH predefinida. El valor HASH es desencriptado después con la clave secreta. El cifrado así obtenido constituye la firma electrónica. La clave pública perteneciente al par de claves puede ser empleada para la verificación de la autenticidad de la firma, siendo generado de nuevo el valor HASH a partir del documento y descifrada la firma electrónica con la clave pública. Si los dos valores HASH así obtenidos coinciden, entonces la firma electrónica es considerada auténtica.

El marco para el empleo de firmas electrónicas para la zona de la Unión Europea fue establecido por la Directiva 1999/ 93/ CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999 por la que se establece un marco comunitario para las firmas electrónicas. En la República Federal de Alemania esta directiva ha sido implementada por la Ley de Firmas. Si se respeta el marco jurídico de la Ley de Firmas, según §126 a del Código Civil la firma electrónica cualificada es equiparada en gran medida a la firma manuscrita, de manera que incuso el requisito de la forma escrita puede ser satisfecho por una firma electrónica cualificada.

Hasta ahora, sin embargo, el empleo de firmas electrónicas en el tráfico jurídico conlleva diferentes dificultades:

1. Muchas aplicaciones existentes, en particular los llamados sistemas heredados, como por ejemplo sistemas llamados de “planificación de recursos de la empresa” (ERP) no soportan la función de firma electrónica.

2. Los formatos de datos diferentes, como por ejemplo formatos de datos EDIFACT, IDOC, XML, CCG-ASCI o BEMIS dificultan el intercambio de documentos firmados electrónicamente entre diferentes sistemas.

3. La adaptación a procedimientos de firma electrónica requiere inversiones relativamente altas en la tecnología de la información y formación de los empleados.

4. Para algunas aplicaciones es necesaria la creación de un entorno de alta seguridad para la protección de los datos firmados, verificados y/o archivados frente a manipulaciones, lo que igualmente es muy costoso.

Por el documento CA 23 84 944 A1 es conocido un sistema de gestión de documentos que ofrece diferentes servicios, en particular la firma electrónica de documentos.

El documento WO01/82036 A da a conocer un sistema y un procedimiento para la firma, almacenamiento y autenticación de documentos electrónicos mediante criptografía de clave pública. El sistema comprende una agrupación de ordenadores de servicio de documentos que está conectada a través de una red a varios ordenadores de usuario, ordenadores del servidor del propietario de documentos y ordenadores de registro. El propietario de los documentos y el usuario del sistema pueden almacenar documentos electrónicos en un banco de datos encriptado de la agrupación de ordenadores de servicio de documentos o sobre un medio de almacenamiento seguro que esté unido a la agrupación de ordenadores del propietario de documentos. Los usuarios pueden identificarse en el sistema por ejemplo mediante una contraseña y enviar una solicitud de firma a la agrupación de ordenadores del servicio de documentos. Esta agrupación de ordenadores del servicio de documentos lee una clave privada del usuario de un banco de datos de la agrupación y firma el documento con esta clave privada. El sistema posibilita a los usuarios de un dispositivo cliente discrecional con acceso a Internet firmar documentos, siendo almacenada la clave privada en páginas de la agrupación de ordenadores de servicio de documentos.

El documento WO03/015370 A da a conocer un sistema y un procedimiento para la firma de datos electrónicos mediante una firma digital. Un servidor central contiene un servidor de firma y un servidor de autenticación. El servidor de firma almacena la clave criptográfica privada de una pluralidad de usuarios. Un usuario puede intercambiar datos con el servidor central a través de una estación de trabajo mediante una unión de túnel segura para por ejemplo transmitir una contraseña o datos de autenticación similares al servidor de autenticación. El servidor de autenticación transmite al servidor de firma un derivado de estos datos de autenticación a través de un canal seguro de transmisión de datos permanente entre estos dos servidores. El derivado es comparado con los datos de autenticación que el usuario ha transmitido directamente al servidor de firma a través del canal seguro de transmisión de datos. Solo cuando de la comparación de datos resulta que el conjunto de datos comparados se corresponden, los datos de usuario son firmados con la clave privada del usuario.

La solicitud de patente DE 10 2005 011 166 no publicada en el momento de la solicitud y la solicitud de patente europea con número de solicitud 06110099 se refieren a un sistema informático con medios para el establecimiento de enlaces de comunicación con varios abonados, medios para la firma de datos que han sido recibidos por uno de

los abonados, medios para la verificación de una firma electrónica de datos que han sido recibidos por uno de los abonados, medios para el archivo de datos que han sido recibidos por uno de los abonados y medios para el almacenamiento de perfiles de abonado, siendo determinado por un perfil de abonado si se deben firmar, verificar y/o archivar los datos recibidos por el abonado en cuestión. Además, en tal sistema informático pueden estar previstos también medios para la conversión de datos a un formato de procesamiento.

Este sistema informático de la solicitud anterior presupone así obligatoriamente que los abonados se registren con sus perfiles de abonado antes de utilizar el sistema informático, definiendo y consignando sus perfiles de abonado respectivos.

La invención se propone por tanto el objeto de conseguir un sistema informático mejorado y un procedimiento para la firma, verificación de la firma y/o archivo de datos, así como también un producto de programa informático correspondiente que facilite el uso de firmas electrónicas en el tráfico jurídico.

Los objetos propuestos por la invención son conseguidos, respectivamente, con las características de las reivindicaciones independientes. Formas de realización preferidas están indicadas en las reivindicaciones dependientes.

Según la invención se consigue un sistema informático que presenta medios para el establecimiento de enlaces de comunicación con varios abonados, medios para la firma de datos recibidos por un abonado a través de una primera función, medios para la verificación de una firma electrónica de datos recibidos por un abonado a través de una segunda función, medios para el archivo de los datos recibidos por un abonado por una tercera función y medios para el reenvío de datos a otro abonado a través de una cuarta función. El sistema informático tiene además medios para la provisión de métodos, siendo definido cada uno de los métodos por al menos una de las primera a cuarta funciones o por una concatenación secuencial y/o paralela de varias de la primera a la cuarta funciones, así como medios para posibilitar una llamada a los métodos por el abonado a través de los enlaces de comunicación.

Por la invención se consigue pues una plataforma que mediante sistemas informáticos externos posibilita a diferentes abonados solicitar servicios que están relacionados con la firma electrónica sin que los abonados tengan que acometer modificaciones esenciales en sus sistemas de tratamiento de la información existentes, por ejemplo aplicaciones ERP. Estos servicios diferentes que son proporcionados por el sistema informático pueden ser requeridos por los abonados a discreción por la llamada a los métodos correspondientes. Cada uno de los métodos incluye así una o varias de las funciones básicas implementadas por el sistema informático.

En cuanto a las funciones básicas se trata de funciones elementales que son necesarias para el manejo de documentos en el tráfico jurídico electrónico, como por ejemplo una función para la firma de datos, una función para la verificación de una firma electrónica, una función para el archivo de datos, una función para el reenvío de datos a través de un medio de comunicación específico y/o otras funciones, como por ejemplo una función para la compresión de datos y una función para la conversión de datos, por ejemplo a un formato de procesamiento y/o a un formato de receptor deseado. Por la definición de métodos estas funciones básicas son agrupadas para formar servicios prácticos.

En el caso más fácil puede ser realizado un método mediante una única función básica, como por ejemplo por la función básica para la firma de datos. La conversión de datos puede ser seleccionada por los abonados como métodos equiparables a la firma, verificación y archivo. Sin embargo, no está prevista en todos los casos.

No obstante, un método puede estar formado también por varias de las funciones básicas. Por una concatenación secuencial y/o paralela de tales funciones básicas y/o otras funciones mediante un método puede ser definido un flujo de trabajo más o menos complejo.

Por ejemplo por uno de los métodos puede ser proporcionado un servicio a través del cual en primer lugar sean firmados los datos, para a continuación archivarlos y enviarlos por correo electrónico a otro abonado. Las funciones básicas para el archivo y el reenvío por correo electrónico pueden así ser procesadas sucesiva o simultáneamente según la definición del método.

Además puede estar definido por ejemplo otro método según el cual en primer lugar se realice la firma de datos y a continuación la verificación de la firma electrónica en el sentido de una llamada verificación de conexión para que la verificación no tenga que ser realizada por el otro abonado que debe recibir los datos firmados. Después de la verificación de conexión sigue la función básica para el reenvío de datos por correo electrónico.

De acuerdo con la Ley de Firma alemana y otras disposiciones relevantes, el proveedor del servicio de firma puede acometer la verificación de conexión solo cuando esta se realiza separada del servicio de firma en cuanto a proceso y personas. Puesto que el sistema informático según la invención puede efectuar tal separación, concretamente por realización separada de las funciones básicas “firma” y “verificación”, el proceso completo se simplifica considerablemente, ya que si no el receptor de la factura tiene siempre el obstáculo de la verificación, lo que puede conducir a que algunos receptores rechacen en general facturas firmadas electrónicamente.

Otro método puede ser definido utilizando la función básica para la verificación de una firma electrónica.

Otro método puede ser definido para la verificación de una firma electrónica y el archivo posterior de los datos, etc.

El sistema informático proporciona pues a los abonados diferentes servicios predefinidos a través de enlaces de comunicación que pueden ser utilizados por llamadas a métodos correspondientes a discreción por los usuarios.

Especialmente ventajoso es que en caso de demandas modificadas o adicionales a los servicios por parte de los abonados puedan ser proporcionados los servicios correspondientes por el sistema informático con mínimo esfuerzo, siendo definidos allí métodos modificados o adicionales correspondientes. Bajo ciertas circunstancias puede ser necesario implementar otras funciones básicas en el sistema informático de las que puedan hacer uso los métodos. Así el sistema informático según la invención constituye una solución muy flexible para las necesidades de los abonados que existen en relación con la firma electrónica.

Según una forma de realización de la invención la interfaz de comunicación del sistema informático según la invención está realizada de manera que las llamadas a métodos puedan realizarse por llamadas a función remota (RFC) por el abonado.

Según una forma de realización de la invención los servicios del sistema informático son proporcionados a los abonados a través de un servicio web. El servicio web corresponde así preferentemente a uno de los estándares de servicios web desarrollados por el consorcio World Wide Web (W3C), en particular también una tecnología de web semántica.

En una forma de realización de la invención la llamada a los métodos proporcionados por el servicio web se realiza por parte del abonado mediante mensajes de Protocolo Simple de Acceso a Objetos (SOAP). A través de estos mensajes son transmitidos en particular también los parámetros para las llamadas a los métodos, así como los datos y/o firmas electrónicas en los métodos respectivos.

Según una forma de realización de la invención los métodos proporcionados por el servicio web se describen con ayuda del Lenguaje de Descripción de Servicios Web (WSDL). Los abonados pueden conocer esta descripción de los métodos proporcionados por el servicio web por la llamada a un documento WSDL correspondiente por el servicio web.

Sobre esta base un abonado puede configurar por ejemplo su sistema ERP de manera que pueda ser interoperable con los métodos proporcionados por el servicio web. Esto puede hacer necesario intervenciones manuales en el sistema ERP del abonado o también realizarse parcial o totalmente de forma automática, en particular si el sistema ERP del abonado presenta una interfaz conforme a W3C.

Según una forma de realización de la invención el documento WSDL está almacenado en un directorio externo para facilitar la localización del servicio web proporcionado por el sistema informático y sus servicios. Así, por ejemplo, puede ser empleado DISCO (Descubrimiento de servicios web). Entonces un abonado puede enviar un documento llamado de descubrimiento a un servidor de directorio externo que a continuación realiza una consulta en un directorio para un servicio web adecuado. Si este es encontrado, el servidor de directorio responde con el documento WSDL del servidor web en cuestión, aquí también con el documento WSDL del servicio web ofrecido por el sistema informático según la invención. Para el descubrimiento de servicios web mencionado puede ser empleado el Protocolo Universal de Descripción, Descubrimiento e Integración (UDDI). La especificación de UDDI puede ser requerida en www.uddi.org.

Según una forma de realización de la invención por el sistema informático son efectuadas también conversiones de formato. Los datos recibidos por un sistema informático externo de un abonado que están en un formato del emisor son convertidos por el sistema informático a un formato de procesamiento empleado por el sistema informático, por ejemplo a un formato de un lenguaje de marcas (llamado “mark-up language”), en particular un formato XML canónico.

Preferentemente para la comunicación entre el sistema informático y un sistema informático externo de un abonado se realiza un acoplamiento máquina-máquina que posibilite un procesamiento completamente automatizado.

Alternativa o adicionalmente a los servicios web la comunicación puede realizarse por ejemplo también mediante correo, FTP, sFTP, OFTP, AS1, AS2. AS3, RosettaNet, telebox400. Los datos a ser procesados pueden ser transmitidos como .pdf, .tiff, .jpg, .doc, .xls, EDIFACT, ASCII, IDS, XML, SAP IDOC, ANSI X.12 o FORTRAS desde el sistema informático externo al sistema informático, pudiendo ser convertidos los datos estructurados también a otro formato estructurado o no estructurado.

Si los datos van a ser reenviados a un receptor que precisa de otro formato de datos, los datos son convertidos desde el formato de procesamiento al formato de receptor deseado. El uso de un formato de procesamiento único por el sistema informático tiene la ventaja de que con ello se puede reducir de forma drástica el número de funciones de conversión. Si el sistema informático debe soportar por ejemplo un número n de formatos de emisor y un número m de formatos de receptor, serían necesarios n x m conversores para la conversión de cada formato de emisor a cada formato de receptor. Por la invención el número de conversores se reduce a un máximo de n + m.

Según una forma de realización de la invención un abonado y/o un sistema informático externo que utiliza el abonado deben autentificarse frente al sistema informático antes de la utilización de los servicios proporcionados por el sistema informático. Para ello se emplea preferentemente un procedimiento de autenticación con un protocolo criptográfico, como por ejemplo el protocolo de Capa de Conexión Segura Versión 3 (SSLV3). La comunicación asegurada entre el sistema informático externo del abonado y el sistema informático según la invención se realiza por ejemplo con ayuda de un certificado. El certificado posibilita una autenticación del abonado y/o de su sistema informático externo frente al sistema informático, así como la comunicación con el sistema informático a través de una conexión segura, como por ejemplo HTTPS. Por ejemplo el certificado es emitido por el explotador del sistema informático, ya que el sistema informático se encuentra preferentemente de todos modos en un llamado centro de confianza, esto es un entorno especialmente seguro que satisface los requisitos legales para la emisión de certificados.

La transmisión de datos entre los sistemas informáticos externos de los abonados y el sistema informático se realiza preferentemente a través de un protocolo de datos, como por ejemplo TCP/IP, como por ejemplo HTTPS, Telebox 400 o una conexión de túnel asegurada de una red privada virtual (VPN).

Según una forma de realización de la invención el sistema informático ofrece la posibilidad de convertir datos de un formato de emisor de un abonado a un formato del receptor de otro abonado. Así los datos recibidos por un abonado son convertidos en primer lugar a un formato XML canónico y a continuación al formato de receptor de otro de los abonados. Para ello puede ser necesaria una adaptación individual del sistema informático para el abonado emisor si este emplea un formato de emisor especial. En tal adaptación son desarrollados métodos de conversión individuales para el cliente que de ahí en adelante mantiene preparado el sistema con una identificación determinada. Tras la adaptación se les proporcionan a los abonados los métodos correspondientes. El abonado que emite llama a los métodos para la conversión de sus datos con ambas identificaciones. La primera identificación determina la conversión de los datos del abonado que emite desde su formato de datos al formato de datos empleado por el sistema informático (XML canónico), la segunda identificación determina la conversión desde el formato de datos empleado por el sistema informático al formato del receptor.

Según una forma de realización de la invención el sistema informático tiene varios puertos de Protocolo de Control de Transmisión (TCP), estando asignado a cada puerto un formato de emisor. Por ejemplo, son empleadas direcciones de puerto libres en el rango de los cinco dígitos. Una dirección de puerto es asignada por ejemplo al formato EDIFACT, otra dirección de puerto al formato IDOC y otra dirección de puerto al formato CCG-ASCI. Si un abonado utiliza por ejemplo el formato EDIFACT, entonces el abonado envía su demanda (solicitud) a la dirección de puerto del sistema informático asignada al formato EDIFACT. A este puerto está asignado un programa de conversión que lleva a cabo la conversión de EDIFACT al formato de procesamiento empleado por el sistema informático.

Según una forma de realización de la invención los abonados son autenticados con ayuda de certificados. Estos certificados de abonado pueden definir limitaciones, por ejemplo en cuanto a determinados empleados del abonado y sus autorizaciones. Para ello determinados campos en el certificado están dotados de informaciones que pueden ser evaluadas por el sistema informático y que pueden servir por ejemplo para instalar limitaciones de acceso para determinadas personas y círculos de personas por ejemplo a determinados periodos de tiempo o expedientes de archivo. Los abonados pueden por tanto gestionar sus propios perfiles de acceso por parte del abonado. Los datos son enviados al receptor por correo electrónico, o este los adquiere por acceso al archivo.

Según una forma de realización de la invención con la ayuda de datos de autenticación de un abonado se accede a su perfil de abonado. Por ejemplo, al abonado se le asigna una identificación de abonado que es empleada como clave para acceder al perfil de abonado en un banco de datos de configuración. En el banco de datos de configuración están almacenados parámetros específicos del abonado que por tanto no tienen que ser transmitidos de nuevo como parámetros en cada llamada al método.

Según una forma de realización de la invención los datos recibidos por un abonado contienen una identificación de otro abonado al que deben ser transmitidos los datos. Con ayuda de esta identificación puede accederse al perfil de abonado del otro abonado para por ejemplo leer el formato de datos deseado por el otro abonado, el tipo de reenvío de los datos al otro abonado- por ejemplo por medios electrónicos o como impresión, así como la dirección del otro abonado.

Un primer abonado que quisiera enviar una factura electrónica a un segundo abonado llama al método correspondiente del sistema informático (firmar, verificar y envío por correo electrónico). Si el abonado quisiera además archivar, entonces llama a otro método correspondiente del sistema informático (firmar, verificar, archivar y envío por correo electrónico). En ambos métodos el primer abonado al llamar al método indica la dirección de correo electrónico del abonado que recibe. Otra posibilidad es que el abonado que recibe recoja (extraiga) el mismo la factura del archivo a través de un método del sistema informático (recuperar archivo).

Los datos recibidos en el formato de datos del primer abonado son convertidos al formato de datos (XML canónico) empleado por el sistema informático. A continuación se realiza la conversión de los datos del formato (XML canónico) empleado por el sistema informático al formato de datos especificado por el segundo abonado, es decir el

formato del receptor, así como la firma electrónica de los datos convertidos al formato del receptor. La firma puede ser realizada por una firma electrónica del explotador del sistema informático, en particular en un procedimiento llamado de firma masiva. Para ello es necesario que el primer abonado haya otorgado al explotador del sistema informático plenos poderes para la firma de sus facturas electrónicas. El abonado otorga plenos poderes en el contrato con el explotador. Solo entonces recibe un certificado correspondiente con el que el abonado puede llamar a los métodos deseados.

En caso de que el primer abonado no haya otorgado tales plenos poderes, los datos convertidos al formato del receptor son transmitidos al primer abonado, de manera que este con un Cliente de Firma puede efectuar el mismo la firma electrónica. Los datos firmados por el primer abonado son después transmitidos al sistema informático y desde allí reenviados al segundo abonado. Además los datos son archivados por el sistema informático cuando el primer abonado lo provoca por la llamada al método correspondiente.

Según una forma de realización de la invención el componente de firma está diseñado para la realización de un procedimiento de firma masiva paralelizado y tiene medios para la distribución de carga dinámica (el llamado “balanceado de carga”) entre las tarjetas con chip que están previstas para la generación de las firmas electrónicas. Por “procedimiento de firma masiva paralelizado” se entiende aquí cada procedimiento de firma en el que la generación de las firmas electrónicas es realizada simultáneamente por varias tarjetas con chip.

Según una forma de realización de la invención son formadas una o varias colas para las ejecuciones de llamadas a la primera función para la generación de firmas electrónicas. Con ello se realiza un paralelizado de la generación de las firmas electrónicas.

Para la generación de la firma masiva sirve un dispositivo de firma masiva que contiene por ejemplo un compartimento para tarjetas con chip con varias tarjetas con chip. Cada una de las tarjetas con chip está diseñada para la generación de una firma electrónica. La asignación de los elementos de una cola a una de las tarjetas con chip se realiza por un llamado planificador.

El planificador puede implementar un procedimiento para la distribución de carga dinámica, es decir para el llamado balanceo de carga, para emplear de la forma más eficaz posible las tarjetas con chip disponibles para la ejecución de las firmas electrónicas.

Por la formación de una cola y la asignación de elementos de la cola a las tarjetas con chip del dispositivo de firma masiva con ayuda de una distribución de carga dinámica se consigue una paralelización del procedimiento de firma masiva que posibilita un rendimiento alto con un número relativamente pequeño de tarjetas con chip.

Según una forma de realización de la invención para las tarjetas con chip del dispositivo de firma masiva está definida una secuencia predeterminada. Cada una de las tarjetas con chip tiene un primer y un segundo estado. En el primer estado la tarjeta con chip está preparada para la recepción de un comando de tarjetas con chip para la generación de una firma electrónica, es decir, está disponible para el procesamiento de un elemento de la cola. En el segundo estado la tarjeta con chip, por el contrario, está “ocupada”, es decir no está disponible al menos temporalmente para la recepción de un elemento de la cola para la generación de una firma electrónica, puesto que la tarjeta electrónica por ejemplo genera tal firma electrónica en ese momento para un elemento de la cola ya asignado antes a la tarjeta con chip. Tan pronto como la tarjeta con chip ha generado tal firma electrónica, emite una señal correspondiente al planificador, de manera que este ajusta el estado de la tarjeta con chip del segundo estado (“ocupada”) al primer estado (”libre”).

El planificador está diseñado por ejemplo, de manera que un elemento de la cola que está en su turno es asignado a una de las tarjetas con chip que presentan en ese momento el primer estado. La asignación a una de las tarjetas con chip que presentan el primer estado puede así realizarse en la secuencia predeterminada de las tarjetas con chip. Si por ejemplo diez tarjetas con chip con los números correlativos 1 a 10 están disponibles en el dispositivo de firma masiva para el procesamiento de la cola y de estas diez tarjetas con chip, las tarjetas con chip 2, 4, 7 y 8 presentan en un instante determinado el primer estado “libre”, entonces el planificador asigna el siguiente elemento de la cola a las tarjetas con chip libres en la secuencia indicada por el número correlativo de las tarjetas con chip, es decir, en el ejemplo considerado asignaría el siguiente elemento de la cola a la tarjeta con chip número 2. El siguiente elemento de la cola sería asignado a la tarjeta con chip 4 y el siguiente elemento de la cola a las tarjetas con chip 7 y 8.

Según una forma de realización de la invención el planificador tiene un componente de tiempo límite que está realizado de manera que una tarjeta con chip que permanece en el segundo estado más de un periodo de tiempo determinado es eliminada de la secuencia de tarjetas con chip. Esto significa que tal tarjeta con chip, por ejemplo debido a un defecto, es considerada al menos temporalmente como no disponible.

Si por ejemplo dentro del periodo de tiempo predeterminado después de que un elemento de la cola ha sido asignado a una tarjeta con chip, esta tarjeta con chip no devuelve ninguna señal al planificador, lo que indica que ha sido generada la firma electrónica para el elemento de la cola en cuestión, entonces esta tarjeta con chip es eliminada lógica y físicamente de la secuencia predeterminada de tarjetas con chip y el elemento de la cola asignado anteriormente a esta tarjeta con chip es asignado a otra tarjeta con chip que permanece en la secuencia predeterminada de tarjetas con chip, de manera que puede ser generada la firma electrónica.

En una forma de realización de la invención se forman al menos dos primera y segunda colas diferentes. Por ejemplo un primer abonado ha otorgado al explotador del sistema informático plenos poderes para la firma de documentos con la firma electrónica del primer abonado. Para la generación de firmas del primer abonado está disponible una primera cantidad de tarjetas con chip en el dispositivo de firma masiva. La primera cola es formada exclusivamente para llamadas a la primera función que vienen del primer abonado. La asignación de elementos de la primera cola por el planificador se realiza solo en tarjetas con chip de la primera cantidad, ya que solo estas tarjetas con chip pueden generar las firmas del primer abonado.

Por el contrario es formada una segunda cola para llamadas a la primera función por varios segundos abonados diferentes que han dado al explotador del sistema informático plenos poderes para la firma de sus documentos con la firma electrónica de un tercero, es decir, por ejemplo la firma electrónica del explotador del sistema informático. En el dispositivo de firma masiva está disponible una segunda cantidad de tarjetas con chip que están diseñadas para la generación de firmas electrónicas del explotador del sistema informático. Los elementos de la segunda cola son asignados por el planificador solo a la segunda cantidad de tarjetas con chip, pero no a la primera cantidad de tarjetas con chip.

Alternativa o adicionalmente pueden ser formadas también colas para abonados individuales o grupos de abonados que desean tipos determinados de firmas electrónicas, como por ejemplo una firma masiva simple, avanzada o cualificada.

La invención posibilita además la verificación y archivo de datos que presentan una firma electrónica. El sistema informático recibe de uno de los abonados datos que presentan una firma electrónica. Para ello el abonado llama al método correspondiente, por ejemplo por un mensaje SOAP. A continuación es verificada la firma electrónica. El curso del procedimiento de verificación es retenido en un protocolo de verificación. Los datos son archivados junto con el protocolo de verificación. Opcionalmente los datos no firmados por el sistema informático son enviados de vuelta al abonado.

Preferentemente el abonado puede acceder al protocolo archivado para asegurarse que la firma electrónica de los datos enviados antes pudo ser verificada. Este acceso puede ser realizado también por otro abonado autorizado a ello. Para eso el sistema informático tiene por ejemplo una interfaz web, de manera que también aquí terceros autorizados a ello puedan acceder cómodamente a los protocolos de comprobación archivados.

Según otra forma de realización de la invención los abonados pueden acceder ellos mismos a sus perfiles de abonado, por ejemplo para actualizarlos. Este acceso puede realizarse por ejemplo mediante una interfaz web del sistema informático. En particular para el caso de aplicación del envío de facturas electrónicas esto tiene la ventaja de que el receptor de la factura puede el mismo actualizar sus datos maestros, de manera que el emisor de la factura no tiene que recibir en primer lugar datos maestros modificados de sus receptores de facturas para después actualizar estos en la memoria de configuración del sistema informático. Preferentemente, sin embargo, por el sistema informático no son almacenados tales perfiles de abonado, sino transferidos todos los parámetros necesarios para la prestación de un servicio deseado por el abonado al sistema informático por la llamada al método correspondiente, por ejemplo con un mensaje SOAP. No obstante, según el caso de aplicación puede estar almacenada una cantidad parcial de los parámetros también en un perfil de abonado. Es posible también configurar el sistema informático de manera que un abonado pueda requerir opcionalmente los servicios con o sin perfil de abonado.

La presente invención es especialmente ventajosa puesto que posibilita crear una plataforma que puede ser requerida por una pluralidad de abonados para servicios relacionados con la firma electrónica. El sistema informático según la invención puede también estar realizado como un llamado “concentrador”. Con ello los gastos totales para inversiones en hardware y software de ordenadores por parte de los abonados se reducen notablemente, ya que también en particular las aplicaciones llamadas heredadas pueden ser interoperables con un sistema informático según la invención.

A continuación se explican en detalle formas de realización preferidas de la invención con referencia al dibujo. Muestran:

Figura 1, un diagrama de bloques de una primera forma de realización de un sistema informático según la invención,

Figura 2, una segunda forma de realización de un sistema informático según la invención,

Figura 3, una forma de realización de un procedimiento según la invención,

Figura 4, una tercera forma de realización de un sistema informático según la invención,

Figura 5, una segunda forma de realización de un procedimiento según la invención,

Figura 6, un diagrama de bloques de una forma de realización de un componente de firma diseñado para la realización de un procedimiento de firma masiva, y

Figura 7, una forma de realización de un procedimiento de firma masiva según la invención.

La figura 1 muestra un sistema informático 100 por medio del cual se proporciona una plataforma para varios abonados I, II, …. El sistema informático 100 tiene una interfaz de comunicación 102 para el establecimiento de enlaces de comunicación con los abonados I, II, ….con ayuda de un protocolo de datos, como por ejemplo TCP/IP. El sistema informático 100 tiene un componente de autenticación 104 para la autenticación de los abonados I, II, …. frente al sistema informático 100. La autenticación se realiza preferentemente empleando un protocolo criptográfico, en particular con el Protocolo de Capa de Conexión Segura (SSL) V3.

El sistema informático 100 tiene un componente de firma 106 para la generación de una firma electrónica, un componente de verificación 108 para la comprobación de la autenticidad de una firma electrónica y un componente de archivo 110 para archivar datos o ficheros, como por ejemplo facturas electrónicas y los protocolos de comprobación correspondientes que fueron generados por el componente de verificación 108.

El componente de conversión 112 del sistema informático 100 sirve para la conversión de los formatos de los datos o ficheros recibidos a un formato de procesamiento empleado por el sistema informático 100. Por ejemplo el sistema informático 100 puede recibir datos en formato EDIFACT, IDOC, CCG-ASCI y/o otros formatos. Los datos de tales formatos son convertidos a un formato único empleado por el sistema informático 100. En cuanto a este formato empleado por el sistema informático 100 puede tratarse por ejemplo de un formato de un lenguaje de marcas, como por ejemplo un formato XML.

Por el componente de conversión 112 puede realizarse también una conversión del formato empleado por el sistema informático 100, esto es por ejemplo el formato XML, a diferentes formatos de receptor de los abonados que puedan recibir datos o ficheros del sistema informático. Tal conversión de datos tiene la ventaja de que independientemente de los formatos de datos de los abonados empleados en cada caso puede realizarse un intercambio de datos entre los abonados a través de la plataforma o “concentrador” formado por el sistema informático 100.

El sistema informático 100 tiene además un componente de reenvío 113 para el reenvío de datos que han sido recibidos por uno de los abonados a otro de los abonados a través de un medio de comunicación especificado, por ejemplo por correo electrónico. El sistema informático 100 puede presentar un componente de reenvío 113 separado para cada medio de comunicación en cuestión. Alternativamente el componente de reenvío 113 puede cubrir diferentes medios de comunicación.

El sistema informático 100 tiene además un componente de análisis 114 para la lectura de informaciones de los datos o ficheros convertidos antes al formato empleado por el sistema informático 100. Tal lectura de informaciones puede ser necesaria para reprocesamiento o reenvío de datos o ficheros. El componente de análisis 114 está diseñado asimismo de manera que puede procesar los datos o ficheros en el formato empleado por el sistema informático 100. La conversión de formato por el componente de conversión 112 tiene pues también la ventaja de que puede emplearse el mismo componente de análisis 114 para procesar datos o ficheros de diferentes abonados que usen diferentes formatos de datos. Esto reduce significativamente el gasto de programación para el componente de análisis 114.

Por el componente de firma 106, el componente de verificación 108, el componente de archivo 110 y el componente de conversión 112 son implementadas funciones básicas correspondientes para la firma, verificación, archivo o conversión. Alternativa o adicionalmente el sistema informático 100 puede implementar otras funciones básicas en relación con el tráfico jurídico electrónico, como por ejemplo una función para la compresión de datos de documentos, por ejemplo una función zip.

Con ayuda del componente de configuración 116 son definidos diferentes métodos basándose en estas funciones básicas. Cada método contiene así al menos una de las funciones básicas. Un método puede también incluir varias de las funciones básicas que estén concatenadas entre sí para formar un flujo de trabajo. La concatenación puede asimismo ser realizada de forma secuencial y/o paralela.

Por ejemplo, un método M1 que es proporcionado por el sistema informático 100 está definido en el componente de configuración 116 como la concatenación secuencial de las funciones básicas proporcionadas por el componente de firma 106 y el componente de reenvío 113.

Correspondientemente se comporta para el método M2 que consiste en una concatenación secuencial de las funciones básicas proporcionadas por el componente de firma 106, el componente de archivo 110 y el componente de reenvío 113. Alternativamente el método M2 puede ser definido también de forma que tras la realización de las funciones básicas proporcionadas por el componente de firma 106 se sucedan paralelas entre sí las siguientes de las funciones básicas proporcionadas por el componente de archivo 110 o el componente de reenvío 113. El componente de configuración 116 incluye otras de tales definiciones para los métodos M3, M4, M5, …, que son proporcionadas por el sistema informático 100.

El componente 116 puede ser mantenido por un administrador para adaptarlo a las necesidades respectivas, por ejemplo para definir métodos adicionales que se basen en las funciones básicas predeterminadas y/o modificar las definiciones existentes.

Los métodos del sistema informático 100 así definidos pueden ser llamados por los abonados a través de la red 126 mediante la interfaz de comunicación 102. Los métodos pueden formar parte del protocolo de datos de la interfaz de comunicación 102 o estar montados antes o después de ella.

Preferentemente la interfaz de comunicación 102 está implementada como servicio web. En este caso las llamadas a los métodos de los abonados se realizan a través del servicio web que contiene estos métodos proporcionados por la interfaz de comunicación 102.

Por la llamada a determinados métodos un abonado puede él mismo determinar cuál de los servicios proporcionados por el sistema informático 100 quiere utilizar. Al llamar a un método, el abonado en cuestión transmite típicamente determinados parámetros que necesita el método para la ejecución del servicio correspondiente, como por ejemplo un parámetro para la especificación de un formato de fichero, una identificación para la conversión, una dirección de correo electrónico para el reenvío, por ejemplo a un receptor de facturas, etc. Además con una llamada a un método puede ser transferida como parámetro una identificación de abonado del receptor de un documento, de manera que los datos en cuestión sean archivados con esta identificación de abonado. El abonado en cuestión puede entonces llamar a los datos archivados en el archivo con ayuda de su identificación de abonado por llamada a un método correspondiente.

Los métodos proporcionados por el sistema informático 100 y los parámetros necesarios para estos métodos pueden estar descritos en un documento WSDL 102'' del servicio web. Los abonados pueden solicitar el documento WSDL 102'' a través de la red 126 directamente al servicio web que proporciona la interfaz de comunicación 102, o por un servidor de directorio externo en forma del llamado descubrimiento de este servicio web.

Si la definición de los métodos en el componente de configuración 116 es modificada, si por ejemplo es definido un método adicional debido a una demanda correspondiente del cliente, es modificado un método existente o se realiza otra actualización de las definiciones de los métodos, son introducidas las variaciones correspondientes también en el documento WSDL 102''.

Por ejemplo el administrador introduce las modificaciones de la definición de los métodos en primer lugar en el componente de configuración 116. Si el administrador introduce un comando para el almacenamiento de las definiciones modificadas, estas variaciones son introducidas automáticamente en el documento WSDL 102'', de manera que los sistemas informáticos externos de los abonados estén informados de esta variación y puedan llamar a los métodos modificados o adicionales. Además de una actualización automática del documento WSDL 102'' puede realizarse también una actualización automática de la versión.

El sistema informático 100 puede además presentar un banco de datos de configuración en el que estén almacenados los perfiles de abonado. A cada perfil de abonado puede accederse con una identificación ("ID de abonado"). En cuanto a la ID de abonado se trata por ejemplo de una clave llamada primaria o secundaria del banco de datos de configuración 116.

En un perfil de abonado pueden estar almacenadas diferentes informaciones específicas del abonado que luego no tienen que ser transferidas como parámetros en una llamada al método. Por ejemplo, en un perfil de abonado puede estar determinado qué datos o ficheros requiere el abonado en cuestión, cuál es su dirección de abonado y/o el tipo de transmisión de datos deseado por el abonado, es decir, por ejemplo de forma electrónica o en forma de papel.

La figura 1 muestra a modo de ejemplo un sistema informático 118 del abonado I. El sistema informático 118 tiene un programa de aplicación 120, por ejemplo un programa llamado ERP. El programa de aplicación 120 puede generar un fichero 122. En cuanto al fichero 122 puede tratarse por ejemplo de una factura electrónica en formato EDIFACT. El sistema informático 118 tiene además una interfaz de comunicación 124 por la que es realizado un protocolo de datos para poder establecer enlaces de comunicación con el sistema informático 100 a través de una red 126. En cuanto a la red 126 puede tratarse por ejemplo de una red pública, por ejemplo Internet, u otra red informática y/o de telecomunicaciones.

El sistema informático 128 del abonado II tiene un programa de aplicación 130; en este caso puede tratarse igualmente de un programa de aplicación ERP, un programa de contabilidad o similares.

El programa de aplicación 130 sirve para el procesamiento de un fichero 132 que ha sido recibido a través de una interfaz de comunicación 134. La interfaz de comunicación 134 realiza un protocolo de datos para el establecimiento de enlaces de comunicación con el sistema informático 100.

Las interfaces de comunicación 124, 134, … de los abonados están diseñadas de manera que los métodos proporcionados por el sistema informático 100 puedan ser llamados a través de la red 126. Preferentemente los protocolos de datos implementados por las interfaces de comunicación 124, 134, … corresponden a un estándar W3C u otro estándar de Internet. En particular las interfaces de comunicación 124, 134, … están diseñadas para la comunicación a través de mensajes SOAP para realizar llamadas a funciones del servicio web de la interfaz de comunicación 102 y transferir o recibir parámetros y datos o ficheros correspondientes.

Las acciones que se pueden realizar con el fichero 122 las determina el abonado I por la llamada a uno de los métodos del propio sistema informático 100. Las informaciones necesarias, por ejemplo los datos del abonado receptor, esto es por ejemplo del abonado II, son transferidas como parámetros a los métodos llamados. En esta forma de proceder los abonados son absolutamente flexibles, puesto que pueden transferir en cada llamada parámetros individuales.

Para el uso de los servicios proporcionados por el sistema informático 100 el abonado 1 establece con su sistema informático 118 un enlace de comunicación por la interfaz de comunicación 124 a través de la red 126 con el sistema informático 100, es decir su interfaz de comunicación 102. Para ello con ayuda del componente de autenticación 104 del sistema informático 100 se realiza la autenticación del abonado I, por ejemplo según el protocolo SSLV3 u otro protocolo o procedimiento de acceso. El acceso se realiza, por ejemplo, basándose en un certificado mediante HTTPS. Tras conseguirse con éxito la autenticación del abonado I este puede dirigir una llamada a una función de los métodos deseados al servicio web del sistema informático 100.

Debido a la autenticación el abonado I está identificado frente al sistema informático 100. Cuando el abonado I ha llamado a un método que incluye una conversión, el sistema informático 100 tan pronto como reciba el fichero 122 del receptor I, convertirá el fichero 122 mediante el componente de conversión 112 al formato empleado por el sistema informático 100, por ejemplo un formato XML canónico. El fichero 122 convertido al formato empleado por el sistema informático 100 es sometido por el componente de análisis 114 a un análisis en cuanto al contenido; en el caso del ejemplo aquí considerado por el análisis del contenido es determinada la identificación del abonado que debe recibir el fichero del abonado I, esto es, por ejemplo su llamado Número de Localización Internacional ILN.

En una forma de realización del sistema informático con un banco de datos de configuración para los abonados, el sistema informático debido a la autenticación y la identificación del abonado I frente al sistema informático 100 que lleva aparejada puede acceder al perfil de abonado del abonado I en el banco de datos de configuración para desde allí llamar a los parámetros para la realización del método que ha sido llamado.

El fichero 122 convertido al formato empleado por el sistema informático 100 es convertido después por el componente de conversión 112 al formato especificado en el perfil de abonado del abonado II. El formato deseado puede ser especificado por una identificación única. Esta identificación puede haber sido determinada en una adaptación individual al cliente previa, llamada personalización. El fichero 122 convertido al formato del abonado II es firmado electrónicamente por el componente de firma 106.

Esto puede realizarse de manera que la firma electrónica se lleve a cabo por ejemplo en un procedimiento llamado de firma masiva por el explotador de la plataforma 100 si el abonado I le ha otorgado los plenos poderes necesarios para ello.

Tras la recepción del fichero 122 firmado que en caso del ejemplo aquí considerado es igual al fichero 132, el sistema informático 128 puede seguir procesando el fichero 132 por ejemplo mediante el programa de aplicación 130. Para ello típicamente es preciso que sea comprobada por el abonado II la autenticidad del fichero 132 firmado electrónicamente. Para la comprobación de la autenticidad del fichero 132 firmado electrónicamente el abonado II conecta su sistema informático 128 al sistema informático 100 a través de la red 126. A continuación el abonado II es autenticado frente al sistema informático 100 con ayuda del componente de autenticación 104. Cuando el abonado II desea la verificación de los ficheros enviados por el abonado I, llama para ello al método M4 correspondiente. En caso de que además de la verificación desee también el archivo del fichero firmado y del protocolo de verificación respectivo, llama por ejemplo al método M5, que además de la verificación realiza el archivo. La verificación de conexión por el sistema informático tiene como consecuencia una simplificación considerable del flujo de trabajo, ya que el abonado II no tiene que efectuar el mismo la verificación.

El abonado II envía después desde el sistema informático 128 el fichero 132 firmado a través de la red 126 al sistema informático 100. Por el componente de verificación 108 es efectuada una verificación de la autenticidad de la firma electrónica del fichero 132 y generado un protocolo de verificación correspondiente. El fichero 132 es archivado junto con el protocolo de comprobación en correspondencia a los parámetros del abonado II transmitidos en la llamada de método al método M5 por el componente de archivo 110. El resultado de la comprobación de la firma electrónica del fichero 132 puede ser comunicado al abonado II por el sistema informático 100 a través de la red 126. Antes del archivo del fichero 132 este es convertido preferentemente por el componente de conversión 112 al formato de datos empleado por el sistema informático 100.

La figura 2 muestra otra forma de realización. Los elementos de la figura 2 que se corresponden con elementos de la figura 1 están caracterizados con los mismos símbolos de referencia.

En el ejemplo de realización considerado aquí el sistema informático 118 dispone de un Cliente de Firma 136 para la ejecución de firmas electrónicas. Para ello está conectado al sistema informático 118 un aparato lector 138 de tarjetas con chip. En una tarjeta con chip 140 está almacenada la clave privada del abonado I para la ejecución de una firma electrónica a través del Cliente de Firma 136. Por ejemplo la clave privada está almacenada en la tarjeta con chip 140 como parte de un llamado entorno de seguridad personal (PSE). Además de la clave privada

pertenecen al PSE entre otros el llamado certificado. Alternativamente el PSE puede ser almacenado en el sistema informático 118 como fichero encriptado. El uso del PSE está típicamente protegido por una contraseña.

El componente de firma 106 del sistema informático 100 está diseñado para la realización de un procedimiento llamado de firma masiva, es decir de firma automatizada. Para ello el componente de firma 106 tiene un llamado compartimento para tarjetas con chip para el alojamiento de un número grande de tarjetas con chip que trabajan en paralelo para posibilitar un alto rendimiento. En un procedimiento de firma masiva basado en tarjetas con chip, las tarjetas con chip están realizadas de manera que tras introducir correctamente una vez el PIN pueda ser realizado de forma automatizada un número discrecional de firmas electrónicas. Los procedimientos de firma masiva son conocidos como tales en el estado de la técnica, véase por ejemplo “Aspekte der Massensignatur”, Detlef Pühlein, Yvonne Knosowksi (http:/www.secunet.de/download/fachartikel/dach2003_aspekte-der-massensignatur.pdf).

En el ejemplo de realización considerado aquí es empleado como protocolo de datos para la comunicación entre el sistema informático 100 y los sistemas informáticos 118, 128, …, el protocolo TPC/IP, como por ejemplo HTTPS a través del puerto 443.

En el ejemplo de realización considerado aquí el componente de conversión 112 (véase la Fig. 1) contiene dos grupos 112’ y 112’’ de conversores. El grupo 112’ de conversores incluye los conversores 148, 150, 152, ... Cada uno de estos conversores del grupo 112’ de conversores sirve para la conversión de un formato de emisor, es decir uno de los formatos de datos o ficheros recibidos por uno de los abonados I, II, … a un formato empleado por el sistema informático 100. En cuanto al formato empleado por el sistema informático 100 se trata preferentemente del formato de un lenguaje de marcas, en particular de un formato XML.

Por ejemplo el conversor 148 sirve para la conversión de un formato de emisor EDIFACT al formato XML del sistema informático 100, el conversor 150 para la conversión de un formato de emisor IDOC a XML, el conversor 152 para convertir un formato de emisor CCG-ASCI en XML, etc. Cabe señalar que en particular en IDOC hay dialectos específicos del cliente. Cuando deben emplearse tales dialectos, para cada uno de estos dialectos debe ser desarrollado un conversor propio en la fase de adaptación individual al cliente. Cada uno de estos conversores contiene su propia identificación única. Correspondientemente debe procederse con diferentes dialectos de otros formatos (por ejemplo EDIFACT).

A cada uno de los conversores 148, 150, 152, … del grupo 112’ de conversores está asociada asimismo una identificación fija. La identificación determina de qué formato de trata. La identificación es transferida como parámetro del método correspondiente al sistema informático 100. Los datos recibidos son convertidos con el conversor determinado por la identificación, respectivamente, al formato XML (XML canónico) del sistema informático 100.

El grupo 112’’ de conversores contiene varios conversores 154, 156, 158, …. En el ejemplo de realización aquí considerado el convertidor 154 sirve para la conversión desde el formato XML del sistema informático 100 a EDIFACT, el conversor 156 para la conversión desde el formato XML al formato IDOC, el convertidor 158 para el conversión desde el formato XML al CCG-ASCI, etc. En general el grupo 112’ de conversores puede contener un número n conversores para la conversión desde n formatos de emisor al formato de procesamiento del sistema informático 100 y el grupo 112’’ de conversores m conversores para la conversión desde el formato de procesamiento a m formatos de receptor. Asimismo puede ser $n < m$, $n = m$ o también $n > m$.

También la conversión del formato es iniciada preferentemente por una llamada a un método de formateado correspondiente. Asimismo la identificación del conversor deseado es transmitida como parámetro en la llamada al método.

El abonado I con ayuda del método llamado determina por ejemplo que hay que firmar un documento electrónico recibido por el abonado I y reenviarlo a un receptor indicado en el documento electrónico o en los parámetros de los métodos. Además en los parámetros del método llamado puede ser indicado el tipo de firma electrónica. El formato de receptor requerido por el abonado II y la dirección de receptor del abonado II es determinada igualmente en los parámetros de los métodos llamados. Con ayuda de la identificación del formato del receptor es seleccionado el conversor correspondiente para la realización de los métodos de conversión.

La comunicación de los abonados I, II, … con el sistema informático 100 se realiza mediante uno de los protocolos de datos 102’ proporcionados por la interfaz de comunicación, como por ejemplo SOAP.

Un fichero 122 generado por la aplicación 120 del sistema informático 118 contiene un documento electrónico, como por ejemplo una factura electrónica. Si en cuanto a la aplicación 120 se trata de un sistema SAP, entonces el fichero 122 es generado típicamente en formato IDOC. El envío del fichero en formato IDOC se realiza a través de la llamada a los métodos correspondientes (conversión) con indicación de la identificación correspondiente para la conversión del formato IDOC determinado en la fase de la adaptación individual. La identificación es dada como parámetro del método (conversión). De forma correspondiente se comporta para las órdenes de conversión de otros abonados, para los que igualmente fue establecida la identificación de conversor correspondiente en la fase de la adaptación individual.

El fichero 122 es recibido pues por el servicio web del sistema informático 100 a través de una llamada de método y reenviado al conversor 150 por medio del cual se realiza una conversión del formato IDOC al formato XML. Además es necesaria una autenticación del abonado I frente del sistema informático 100 que es realizada por el componente de autenticación 104.

Del método llamado y los parámetros dados resulta que el abonado I desea una conversión a un formato de receptor con firma electrónica subsiguiente del fichero 122 y su reenvío a un abonado identificado en el fichero 122 o en los parámetros.

En una realización del sistema informático a continuación es iniciado el componente de análisis 114 para leer una identificación de receptor a partir del fichero 122, como por ejemplo el ILN del abonado que debe recibir el fichero firmado. El fichero 22 convertido a XLM es convenido acto seguido al formato de receptor por uno de los conversores 154, 156, 158, .. del grupo 112'' de conversores. Si el receptor, por ejemplo el abonado II, requiere el formato EDIFACT, entonces la conversión es efectuada por ejemplo por el conversor 154 que corresponde al dialecto EDIFACT del cliente.

El fichero 122 convertido al formato del receptor es entonces firmado electrónicamente. Esto es realizado por el sistema informático 100 mediante el componente de firma electrónica 106 en un procedimiento de firma masiva.

El sistema informático 100 puede presentar varios puertos TCP/ IP 142, 144, 146, …En una forma de realización de la invención a cada uno de los puertos TCP/ IP está asignado un número de puerto. Por ejemplo, el puerto TCP/ IP142 tiene el número de puerto A, el puerto TCP/ IP 144 el número de puerto B, el puerto TPC/ IP 146 el número de puerto C, etc.

Por ejemplo los números de puerto A, B, C, … están dentro de un rango de números que no contiene los números de puerto en general habituales. Comúnmente los números de puerto habituales son por ejemplo el número de puerto 23 para Telnet, el número de puerto 25 para SMTP, el número de puerto 80 para HTTP, el número de puerto 443 para HTTPS, el número de puerto 3389 para MSRemote Desktop/Servicios de terminal, números de puerto 5631 y 5632 para pcAnywhere. Por ejemplo, los números de puerto A, B, C, … tienen por lo menos cinco cifras y son asignados en orden ascendente a partir del número de puerto 50.000. Además de los puertos TCP/IP 142, 144, 146, … de este rango de números de puerto aún no ocupados el sistema informático 100 puede presentar otros puertos habituales, como por ejemplo un puerto 80 para HTTP y un puerto 443 para comunicación HTTPS .

En la forma de realización aquí considerada a cada uno de los conversores 148, 150, 152, … del grupo 112' de conversores está asignado fijamente uno de los puertos TCP/IP 142, 144, 146, ... En particular el conversor 148 está asignado al puerto TCP/IP 142, el conversor 150 al puerto TCP/IP 144 y el conversor 152 al puerto TCP/IP 146, etc. El puerto TCP/IP 142 sirve así para la recepción de documentos EDIFACT que después son convertidos automáticamente por el conversor 148 asignado al puerto TCP/IP 142 al formato XML del sistema informático 100. Correspondientemente el puerto TCP/IP 144 sirve para la recepción de documentos IDOC, que luego son convertidos automáticamente a XML, el puerto 146 sirve para la recepción de documentos CCG-ASCI que igualmente son convertidos automáticamente al formato XML.

Para el abonado II puede ser almacenado un perfil de receptor en el banco de datos de configuración 116 al que pueda accederse con la identificación del abonado II, es decir, con su "ID de receptor" como clave. El perfil de receptor del abonado II determina el formato de receptor requerido por el abonado II y la dirección de receptor del abonado II.

La comunicación de los abonados I, II con el sistema informático 100 se realiza mediante uno de los protocolos de datos 102' proporcionados por la interfaz de comunicación, mediante el cual pueden ser llamados los métodos M1, M2, M3….

La interfaz de comunicación 124 del sistema informático 118 está aquí configurada de manera que se realiza el envío del fichero 122 al puerto asignado al formato IDOC del sistema informático 100, es decir, al puerto TCP/IP 144 con el número de puerto B. Correspondientemente se comporta para las interfaces de comunicación de los otros abonados, que están configuradas, respectivamente, de manera que se realiza un envío de un fichero al sistema informático 100 a aquel puerto del sistema informático 100 al que está asignado el formato de emisor respectivo.

El fichero 122 es pues recibido por el puerto TCP/IP 144 del sistema informático 100 y reenviado al conversor 150 por el cual se realiza una conversión del formato IDOC a XML.

En una forma de realización del sistema informático es iniciado el componente de análisis 114 para leer una identificación de receptor del fichero 122, como por ejemplo el ILN del abonado que debe recibir el fichero firmado. Con la identificación de receptor así obtenida se accede al perfil de receptor del abonado en el banco de datos de configuración 116 que debe obtener el fichero 122 firmado. Allí es indicado el formato de receptor requerido por el receptor. El fichero 122 convertido a XML es convertido a continuación por un conversor 154, 156, 158, … del grupo 112'' de conversores al formato de receptor. Si el receptor, por ejemplo el abonado II, requiere el formato EDIFACT, entonces se lleva cabo la conversión por el conversor 154.

La figura 3 muestra un diagrama de flujo correspondiente, en el que el tipo de conversión es seleccionado por los abonados mediante llamada a métodos y no por los puertos.

En la etapa 200 se realiza una autenticación de uno de los abonados, por ejemplo del abonado I que funciona como emisor, frente a la plataforma proporcionada por el sistema informático 100 (véanse las figuras 1 y 2). Preferentemente la autenticación se realiza con el protocolo SSLV3 (basado en certificado, HTTPS).

En la etapa 202 se realiza la llamada al método deseado por el abonado I. Con la llamada del método correspondiente y los parámetros transmitidos el abonado I determina, por ejemplo, que el documento recibido debe ser firmado, reenviado a un receptor y archivado (método M1- véanse las figuras 1, 2 y 4).

En la etapa 204 es recibido un documento por el abonado I. En la etapa 206 este es convertido al formato de la plataforma, es decir al formato de procesamiento. En la etapa 208 es leída a partir de los parámetros dados una identificación de receptor "ID de receptor". El formato de receptor determinado por el receptor y la dirección de receptor proceden de los parámetros transmitidos en la llamada al método (es decir se suprime la etapa 210). El documento es convertido después en la etapa 212 al formato del receptor y en la etapa 214 se realiza la firma electrónica del documento convertido, ya sea en un procedimiento de firma masiva a través de la plataforma o tras trasferencia del documento convertido por el propio abonado I.

En la etapa 216 el documento para el abonado I es archivado. Esto puede realizarse en el formato de emisor del abonado I, en el formato de receptor del abonado II o en el formato XML de la plataforma. El archivo puede realizarse en el formato de la plataforma o en otro formato deseado por el abonado en cuestión. Prácticamente debería ser el formato en el que esté el documento válido es decir la factura firmada; además al mismo tiempo es archivado el protocolo de comprobación.

En la etapa 218 el documento convertido y firmado es reenviado al receptor, es decir por ejemplo al abonado II. Según la definición del método llamado puede realizarse una compresión de los datos antes del archivo o reenvío.

La figura 4 muestra otra forma de realización del sistema informático. Los elementos de la figura 4 que corresponden a elementos de las figuras 1 y 2 están caracterizados con los mismos símbolos de referencia. El sistema informático 100 en la forma de realización de la figura 4 tiene además de los puertos TCP/IP 142, 144, 146, …, que están asignado, respectivamente, a un formato de emisor determinado, los puertos estándar 160 y 162 con los números de puerto 80 ó 443 para los protocolos de datos HTTP o HTTPS.

El sistema informático 100 está unido a un llamado centro de confianza 164 o contiene uno de tales. En cuanto al centro de confianza 164 se trata de una entidad de certificación, por ejemplo de acuerdo a la Ley de Firma de la República Federal Alemana. Con ayuda del centro de confianza 164 puede ser verificado si el certificado transferido con la firma electrónica es válido o no.

La figura 4 muestra un sistema informático 166 de un abonado III. El sistema informático 166 tiene un programa de aplicación 168 y una interfaz de comunicación 172 que puede realizar un protocolo de datos, como por ejemplo HTTP o HTTPS. Por el sistema informático 166 puede ser recibido un documento 170 firmado que es almacenado como fichero por la aplicación 168.

Para la verificación de la firma electrónica del documento 170 firmado el abonado III hace uso del sistema informático 100. Para ello se establece entre el sistema informático 166 y el sistema informático 100 un enlace a través de la red 126, por ejemplo mediante HTTP o HTTPS, es decir con el puerto 160 o el puerto 162 del sistema informático 100. Para ello en primer lugar el abonado III es autentificado. Tras la identificación y autenticación del abonado III, el abonado III por llamada a un método deseado, por ejemplo el método M5, con transferencia de los parámetros necesarios puede enviar un documento firmado al sistema informático 100 para verificar el documento en cuanto a su firma y archivar el documento recibido junto con el protocolo de comprobación generado en la verificación de la firma electrónica.

Después de que el sistema informático 100 ha recibido el documento 170 firmado por el abonado III, realiza una comprobación de la autenticidad y la validez de la firma electrónica con ayuda del componente de verificación 108 que para ello accede también al centro de confianza 164 para comprobar la validez del certificado correspondiente a la firma electrónica. Para ello se crea un protocolo de comprobación.

El documento firmado 170 y/o el documento sin firmar 172 son archivados junto con el protocolo de comprobación generado en la verificación por el componente de archivo 110. Por ejemplo se emplea para ello una llamada biblioteca de cintas 174 del sistema informático 100 u otro medio de almacenamiento adecuado para el archivo.

La figura 5 muestra un diagrama de flujo correspondiente.

En la etapa 300 se realiza la autenticación del abonado III, es decir del emisor del documento firmado, frente a la plataforma. El método llamado por el abonado III está definido por ejemplo en el componente de configuración 116 (véanse las figuras 1, 2 y 4), de manera que sean verificados y archivados los datos recibidos por el abonado III. En la etapa 304 es recibido un documento firmado por el abonado III por la plataforma. En la etapa 306 se realiza una

verificación de la firma electrónica del documento y la creación de un protocolo de verificación correspondiente. Tras la comprobación puede realizarse una conversión a un formato deseado por el abonado III si esta función pertenece a la definición del método llamado. El formato deseado por el abonado III puede ser transferido al sistema informático o a su servidor web en forma de una identificación como parámetro en la llamada al método por el abonado III.

Además puede ser empleado uno de los conversores del grupo 112'' de conversores (véase la figura 4) para generar un documento 172 (véase igualmente la figura 4) convertido al formato deseado. En la etapa 310 el documento y su protocolo de comprobación correspondiente son archivados y el documento verificado es transferido al abonado III en la etapa 312 en caso necesario tras la conversión. En la etapa 314 el abonado III puede acceder al protocolo de verificación archivado por ejemplo a través de la interfaz-web de la plataforma. Tal acceso al protocolo de comprobación puede realizarse también por otro abonado autorizado a ello.

La figura 6 muestra un diagrama de bloques de una forma de realización de un componente de firma 106 como puede emplearse por ejemplo en las formas de realización de las figuras 1, 2 y 4. El componente de firma puede formar una o varias colas, como por ejemplo la cola 176 mostrada en la figura 6. La cola 176 opera por ejemplo según el principio "primero en entrar, primero en salir" (FIFO).

El componente de firma 106 contiene además un dispositivo de firma masiva 178 que presenta por ejemplo un compartimento para tarjetas con chip. El dispositivo de firma masiva 178 sirve para el alojamiento de por ejemplo un número n de tarjetas con chip C_j con $0 < j \leq n$. Por los números j correlativos de las tarjetas con chip es definida lógicamente una secuencia de las tarjetas con chip en el ejemplo de realización considerado aquí.

El componente de firma 108 tiene además un planificador 180 para la asignación de los elementos de la cola 176 a las tarjetas con chip C_j del dispositivo de firma masiva 178. Esta asignación puede ser realizada por distribución de carga dinámica entre las tarjetas con chip.

El planificador 180 tiene acceso a los datos de estado 182 de las tarjetas con chip. A cada una de las tarjetas con chip que pueden procesar elementos de la cola 176 es asignado un estado con ayuda de los datos de estado 182 y concretamente un primer estado "libre" o un segundo estado "ocupado".

El primer estado "libre" indica que la tarjeta con chip en cuestión está preparada para la recepción de un comando de tarjeta con chip para la generación de una firma electrónica para un elemento de la cola 176. El estado "ocupado" asociado a una de las tarjetas con chip, por el contrario, indica que la tarjeta con chip en cuestión no está preparada para la recepción de un comando de tarjeta con chip con la demanda para la generación de una firma electrónica para un elemento de la cola, lo que puede ser debido a que la tarjeta con chip en cuestión esté ocupada precisamente en la generación de tal firma electrónica para un elemento de la cola asignado anteriormente a esta tarjeta con chip.

En el momento considerado aquí por ejemplo la tarjeta con chip C1 tiene el estado "ocupado", la tarjeta con chip C2 el estado "libre", la tarjeta con chip C3 el estado "ocupado", la tarjeta con chip C4 el estado "libre", …

El planificador 180 puede presentar un componente de tiempo límite 184. Después de que el planificador 180 ha asignado un elemento de la cola a una de las tarjetas con chip y ha dirigido un comando de tarjeta con chip correspondiente a la tarjeta con chip en cuestión, es iniciado un temporizador del componente de tiempo límite 184. Después de que la tarjeta con chip ha ejecutado el comando de tarjeta con chip, es decir, después de que ha sido generada la firma electrónica, la tarjeta con chip en cuestión responde con la salida de la firma electrónica requerida. Con esto se detiene el temporizador.

Pero si el valor del temporizador alcanza un valor umbral predeterminado que está por encima del tiempo que necesita típicamente la tarjeta con chip para la generación de una firma electrónica, entonces el planificador 180 asume que la tarjeta con chip en cuestión al menos temporalmente no está disponible para la generación de firmas electrónicas, puesto que por ejemplo hay un defecto técnico. La tarjeta con chip en cuestión es eliminada al menos lógicamente de la secuencia predeterminada de tarjetas con chip, de modo que esencialmente ya no está disponible para la asignación de elementos de la cola 176. Esto puede realizarse de manera que la tarjeta con chip en cuestión sea dispuesta permanentemente en el estado "ocupado".

En tal caso cuando el temporizador alcanza un valor umbral predeterminado, el planificador 180 reasigna el elemento de la cola asignado antes a esta tarjeta con chip a otra de las tarjetas con chip que esté incluida en la secuencia predeterminada y que no presente un estado "ocupado" temporal o permanente.

En el funcionamiento el componente de firma 106 recibe una demanda 186 Ai para la generación de una firma electrónica para un documento de un abonado. La demanda Ai produce una llamada a la primera función, es decir la función de firma. La demanda Ai es acoplada al último elemento en la cola 176. Tan pronto como han sido procesados los elementos de la cola 176 que preceden a la demanda Ai, es decir los elementos A1, A2, A3, .., la demanda Ai es asignada por el planificador 180 a una de las tarjetas con chip que tiene en ese momento el estado "libre".

Esto se realiza preferentemente en la secuencia predeterminada de las tarjetas con chip, es decir la demanda Ai es asignada en el instante representado en la figura 6 a la tarjeta con chip C2, ya que aquí se trata de una tarjeta con chip con el mínimo índice j=2. El planificador 180 envía a continuación un comando de tarjeta con chip a la tarjeta con chip C2 para la generación de una firma electrónica correspondiente a la demanda Ai. Al mismo tiempo es actualizado el estado de la tarjeta con chip C2 a los datos de estado 182, concretamente es pasado de “libre” a “ocupado”. Además el temporizador del componente de tiempo límite 184 es iniciado para la tarjeta con chip C2.

Si la tarjeta con chip C2 funciona normalmente, dentro de un periodo de tiempo de por ejemplo aproximadamente un segundo emite la firma electrónica 188 deseada que es expedida por el componente de firma 106 al sistema informático 100. Si, por el contrario, la tarjeta con chip C2 no responde al comando de tarjeta con chip con la salida de la firma electrónica 188 dentro del periodo de tiempo predeterminado por el componente de tiempo límite 184 de por ejemplo 1,5 segundos, entonces el planificador 180 asume que la tarjeta con chip C2 no está disponible al menos temporalmente, de manera que el estado de la tarjeta con chip C2 permanece “ocupado” y la demanda Ai es asignada a otra tarjeta con chip que en ese momento presente el estado “libre” para la generación de la firma electrónica 188 deseada. Con las demandas que siguen a la demanda Ai se actúa según el mismo procedimiento.

La figura 7 muestra una forma de realización de un procedimiento de firma masiva según la invención. En la etapa 400 el planificador accede a la demanda Ai de la cola que está en su turno como siguiente para el procesamiento. En la etapa 402 el planificador asigna esta demanda Ai a una de las tarjetas con chip disponibles para la firma electrónica deseada que tienen el estado “libre”. La asignación de la demanda Ai se realiza asimismo por ejemplo a las tarjetas con chip libres en la secuencia indicada por su número correlativo j. En la etapa 404 la tarjeta con chip Cj, a la que ha sido asignada la demanda Ai en la etapa 402 es pasada al estado “ocupada”. En la etapa 406 es incrementado el índice i, de manera que a continuación sea procesada la siguiente demanda Ai de la cola.

En la etapa 408 que se desarrolla de forma asíncrona respecto a las etapas 400 a 406, el planificador recibe de la tarjeta con chip Cj u otra tarjeta con chip que ha sido asignada antes a un elemento de la cola, la información “tarjeta con chip libre”, después de lo cual el planificador cambia el estado de la tarjeta con chip en cuestión de “ocupada” a “libre”. La información “tarjeta con chip libre” puede venir dada implícitamente por la devolución de una firma por una de las tarjetas con chip, ya que esto significa que la tarjeta con chip puede procesar a continuación otro elemento de la cola.

Para la realización de la firma masiva pueden ser definidas por ejemplo primeras y segundas cantidades de tarjetas con chip a las que estén asignados respectivamente una cola y un planificador. Por ejemplo las tarjetas con chip de la primera cantidad sirven para la generación de firmas electrónicas de un primer abonado. Correspondientemente la cola asignada a la primera cantidad de tarjetas con chip contiene solo demandas que vienen de este primer abonado.

La segunda cantidad de tarjetas con chip del dispositivo de firma masiva 178 sirve por el contrario para la generación de firmas electrónicas de un tercero, por ejemplo del explotador del sistema informático 100. La cola asignada a la segunda cantidad de tarjetas con chip contiene correspondientemente demandas de distintos abonados que han otorgado al explotador del sistema informático 100 plenos poderes para firmar los documentos de este abonado con la firma electrónica del explotador. Además también pueden ser formadas colas dedicadas a determinados tipos de firmas electrónicas, como por ejemplo firmas masivas simples, avanzadas o cualificadas que sean asignadas a cantidades correspondientes de tarjetas con chip, que puedan generar, respectivamente, el tipo deseado de firma electrónica.

Para cada una de estas diferentes opciones pueden ser definidos métodos correspondientes en el componente de configuración 116 (véanse las figuras 1, 2 y 4), por ejemplo un método M6 para la llamada a un flujo de trabajo que incluye una firma masiva con la firma de un abonado determinado. Este método M6 puede también por tanto ser llamado solo por este abonado tras la autenticación previa. Además puede ser definido un método M7 que incluye una firma masiva con la firma electrónica del explotador del sistema informático 100.

Lista de símbolos de referencia

100	Sistema informático
102	Interfaz de comunicación
102’	Protocolo de datos
102’’	Documento WSDL
104	Componente de autenticación
106	Componente de firma
108	Componente de verificación
110	Componente de archivo

112 Componente de conversión

112' Grupo de conversores

112'' Grupo de conversores

114 Componente de análisis

116 Componente de configuración

118 Sistema informático

120 Programa de aplicación

122 Fichero

124 Interfaz de comunicación

126 Red

128 Sistema informático

130 Programa de aplicación

132 Fichero

134 Interfaz de comunicación

136 Cliente de firma

138 Dispositivo de lectura de tarjetas con chip

140 Tarjeta con chip

142 Puerto TCP/IP

144 Puerto TCP/IP

146 Puerto TCP/IP

148 Conversor

150 Conversor

152 Conversor

154 Conversor

156 Conversor

158 Conversor

160 Puerto estándar

162 Puerto estándar

164 Centro de confianza

166 Sistema informático

168 Programa de aplicación

170 Documento firmado

171 Interfaz de comunicación

172 Documento no firmado

174 Biblioteca de cintas

176 Cola

178 Dispositivo de firma masiva

180 Planificador

182 Datos de estado

184 Componente de tiempo límite

186 Demanda

188 Firma electrónica

REIVINDICACIONES

1. Sistema informático con

- medios (102; 102', 102'') para el establecimiento de enlaces de comunicación con varios sistemas informáticos (118, 128; 166) de abonados externos de varios abonados,
- medios (106) de firma de datos que han sido recibidos por uno de los sistemas informáticos de abonados externos a través de una primera función, estando diseñados los medios de firma para la realización de un procedimiento de firma masiva paralelizado,
- medios (176, 180) para la distribución de carga dinámica entre varias tarjetas con chip que están previstas para la generación de las firmas electrónicas,
- medios (108) para la verificación de una firma electrónica de datos que han sido recibidos por uno de los sistemas informáticos de abonados externos a través de una segunda función,
- medios (110) para el archivo de datos que han sido recibidos por uno de los sistemas informáticos de abonados externos a través de una tercera función,
- medios para el reenvío de datos que han sido recibidos por uno de los sistemas informáticos de abonados externos a otro de los sistemas informáticos de abonados externos a través de uno de los enlaces de comunicación por medio de una cuarta función,
- medios (116) para la provisión de métodos (M1, M2, M3,…), estando definido cada uno de los métodos por al menos una de las primera a cuarta funciones o por una concatenación secuencial y/o paralela de varias de las primera a cuarta funciones, y conteniendo al menos algunos de los métodos varias de las funciones primera a cuarta,
- medios para posibilitar la llamada a los métodos por los sistemas informáticos de abonados externos a través de enlaces de comunicación,
- medios (104) para la autenticación de los abonados y/o de los sistemas informáticos de abonados externos, estando diseñados los medios de autenticación para la realización de un protocolo criptográfico con ayuda de un certificado,

en el que la llamada a uno de los métodos por uno de los sistemas informáticos de abonados externos presupone la autenticación previa del abonado de este sistema informático de abonado externo y/o del sistema informático de abonado externo frente al sistema informático.

2. Sistema informático según la reivindicación 1, con medios (112; 112', 112'') para la conversión de datos de un formato de emisor de un primer abonado a un formato del sistema informático y para la conversión de datos del formato del sistema informático a un formato del receptor de un segundo abonado.

3. Sistema informático según la reivindicación 2, en el que los medios para la conversión pueden ser llamados mediante métodos y en el que los medios para la conversión pueden ser configurados específicamente para el abonado y pueden ser llamados por el abonado en cuestión como métodos específicos del abonado mediante una identificación de abonado correspondiente.

4. Sistema según una de las reivindicaciones anteriores, con un servicio web, en el que el servicio web contiene los métodos, en el que el servicio web contiene un documento WSDL que incluye una descripción de los métodos y sus parámetros, pudiendo ser llamado el documento WSDL por los abonados a través de los enlaces de comunicación, estando almacenado un documento WSDL del servicio web que contiene una descripción de los métodos y sus parámetros en un directorio externo desde el cual puede ser llamado por los abonados a través de una red pública.

5. Sistema informático según la reivindicación 4, en el que los medios para la firma presentan medios de cola (176) para la formación de una cola para la ejecución de llamadas de la primera función en base a la llamada de los métodos correspondientes que contienen la primera función, y que comprende también un dispositivo de firma masiva (178) con varias tarjetas con chip, estando diseñada cada una de las tarjetas con chip para la generación de una firma electrónica, y medios de planificador (180) para la asignación de un elemento de la cola que es el siguiente en la fila a una de las tarjetas con chip.

6. Sistema informático según la reivindicación 5, en el que para las tarjetas con chip está definida una secuencia predeterminada y en el que cada tarjeta con chip tiene un primer o un segundo estado, de modo que la tarjeta con chip solo en el primer estado puede procesar un elemento de la cola para la generación de una firma electrónica, y en el que los medios de planificador están diseñados de manera que un elemento de la cola que es el siguiente de la fila es asignado a una de las tarjetas con chip que tiene el primer estado en la secuencia predeterminada de las tarjetas con chip.

7. Sistema informático según la reivindicación 6, en el que los medios de planificador tienen un componente de tiempo límite (184) que están diseñados de manera que una de las tarjetas con chip que permanece en el segundo estado más del periodo de tiempo predeterminado es eliminada de la secuencia predeterminada de tarjetas con

chip, y por que un elemento de la cola asignado previamente a esta tarjeta con chip es reasignado por los medios de planificador a una de las tarjetas con chip que permanecen en la secuencia predeterminada.

8. Sistema informático según una de las reivindicaciones anteriores, con medios para la conversión de los datos recibidos por un abonado a un formato de un lenguaje de marcas y para la conversión de los datos desde el formato del lenguaje de marcas a un formato de receptor, sirviendo el formato de lenguaje de marcas como formato de procesamiento.

9. Procedimiento para la firma, verificación de firma, archivo y/o reenvío de datos mediante un sistema informático, presentando el sistema informático una interfaz para el establecimiento de enlaces de comunicación con varios abonados y pudiéndose realizar a través de la interfaz la llamada a métodos del sistema informático por los abonados, estando definido cada uno de los métodos al menos por una función para la firma, verificación de la firma, archivo y/o reenvío de datos o una concatenación secuencial o paralela de tales funciones, con las siguientes etapas:

- establecimiento de un enlace de comunicación de uno de los abonados con el sistema informático para la recepción de datos del abonado,
- realización de uno de los métodos llamados por el abonado,
- en el que la firma se realiza con un procedimiento de firma masiva paralelizado, realizándose una distribución de carga dinámica entre varias tarjetas con chip de un dispositivo de firma masiva (178), estando diseñada cada una de las tarjetas con chip para la generación de una firma electrónica.

10. Procedimiento según la reivindicación 9, en el que los datos recibidos por uno de los abonados son convertidos al formato de un lenguaje de marcas y/o en el que los datos son recibidos en un puerto del sistema informático al que está asignado el formato de los datos.

11. Procedimiento según la reivindicación 10, en el que el procedimiento de firma masiva paralelizado incluye las siguientes etapas:

- formación de una cola para la realización de las primeras funciones en base a la llamada a los métodos correspondientes que incluyen la primera función,
- asignación del elemento de la cola que es el siguiente de la fila a una tarjeta con chip del dispositivo de firma masiva (178) que contiene varias tarjetas con chip.

12. Procedimiento según la reivindicación 11, en el que para las tarjetas con chip está definida una secuencia predeterminada y en el que cada tarjeta con chip tiene un primer o un segundo estado, de modo que cada tarjeta con chip solo en el primer estado puede procesar un elemento asignado a ella de la cola para la generación de una firma electrónica, y en el que la asignación de un elemento de la cola que es el siguiente de la secuencia se realiza de manera que la asignación de este elemento a una de las tarjetas con chip que tienen el primer estado se realiza en la secuencia predeterminada de tarjetas con chip, y en el que preferentemente una tarjeta con chip que permanece en el segundo estado más del periodo de tiempo predeterminado es eliminada de la secuencia predeterminada de tarjetas con chip, y en el que preferentemente un elemento de la cola asignado previamente a esta tarjeta con chip es reasignado a una de las tarjetas con chip que quedan en la secuencia predeterminada, y/o en el que para un primer abonado es formada una primera cola que contiene solo llamadas a la primera función del primero de los abonados, y en el que para varios segundos abonados es formada una segunda cola común que contiene las llamadas a la primera función por los segundos abonados.

13. Producto de programa informático, en particular medio de almacenamiento digital, con instrucciones ejecutables por ordenador para la realización de un procedimiento según una de las reivindicaciones 9 a 12.

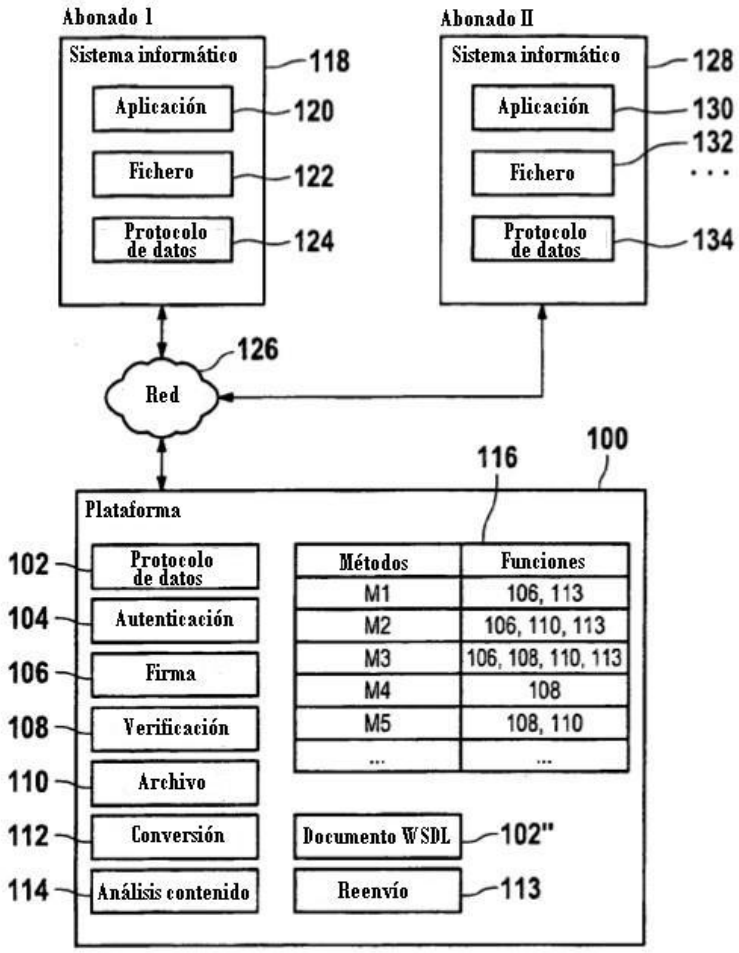
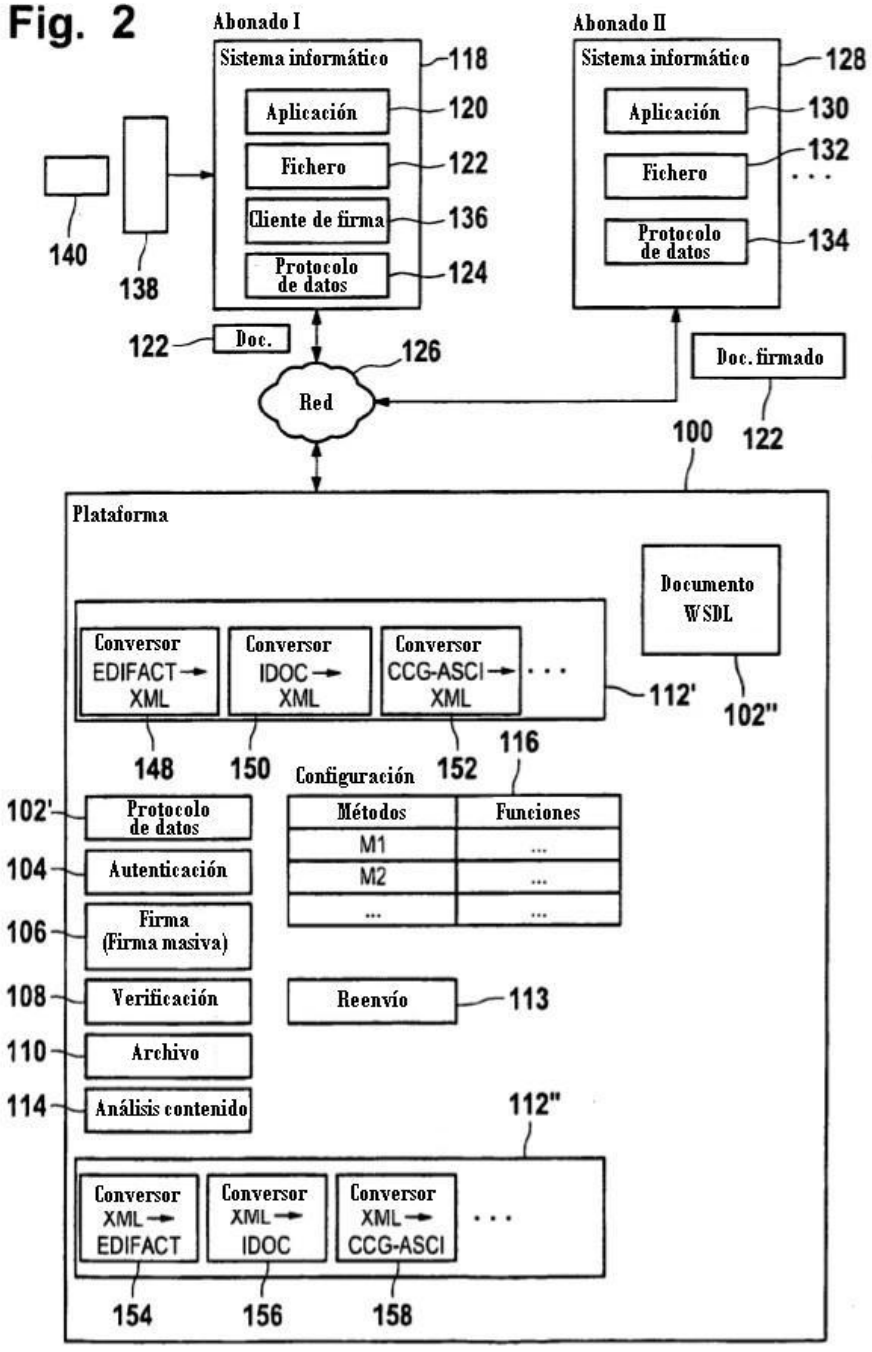

Abonado I
Sistema informático
118
Aplicación
120
Fichero
122
Protocolo de datos
124
Abonado II
Sistema informático
128
Aplicación
130
132
Fichero
Protocolo de datos
134
126
Red
100
116
Plataforma
102
Protocolo de datos
104
Autenticación
106
Firma
108
Verificación
110
Archivo
112
Conversión
114
Análisis contenido
Métodos
Funciones
M1
106, 113
M2
106, 110, 113
M3
106, 108, 110, 113
M4
108
M5
108, 110
Documento WSDL
102"
Reenvío
113

Fig. 1

Fig. 2


Abonado I
Sistema informático
118
Aplicación
120
Fichero
122
Cliente de firma
136
Protocolo de datos
124
140
138
122
Doc.
126
Red
Abonado II
Sistema informático
128
Aplicación
130
Fichero
132
Protocolo de datos
134
Doc. firmado
122
100
Plataforma
Documento WSDL
102"
Conversor EDIFACT → XML
Conversor IDOC → XML
Conversor CCG-ASCI → XML
112'
148
150
152
116
Configuración
Métodos
Funciones
M1
M2
102'
Protocolo de datos
104
Autenticación
106
Firma (Firma masiva)
108
Verificación
Reenvío
113
110
Archivo
114
Análisis contenido
112"
Conversor XML → EDIFACT
Conversor XML → IDOC
Conversor XML → CCG-ASCI
154
156
158

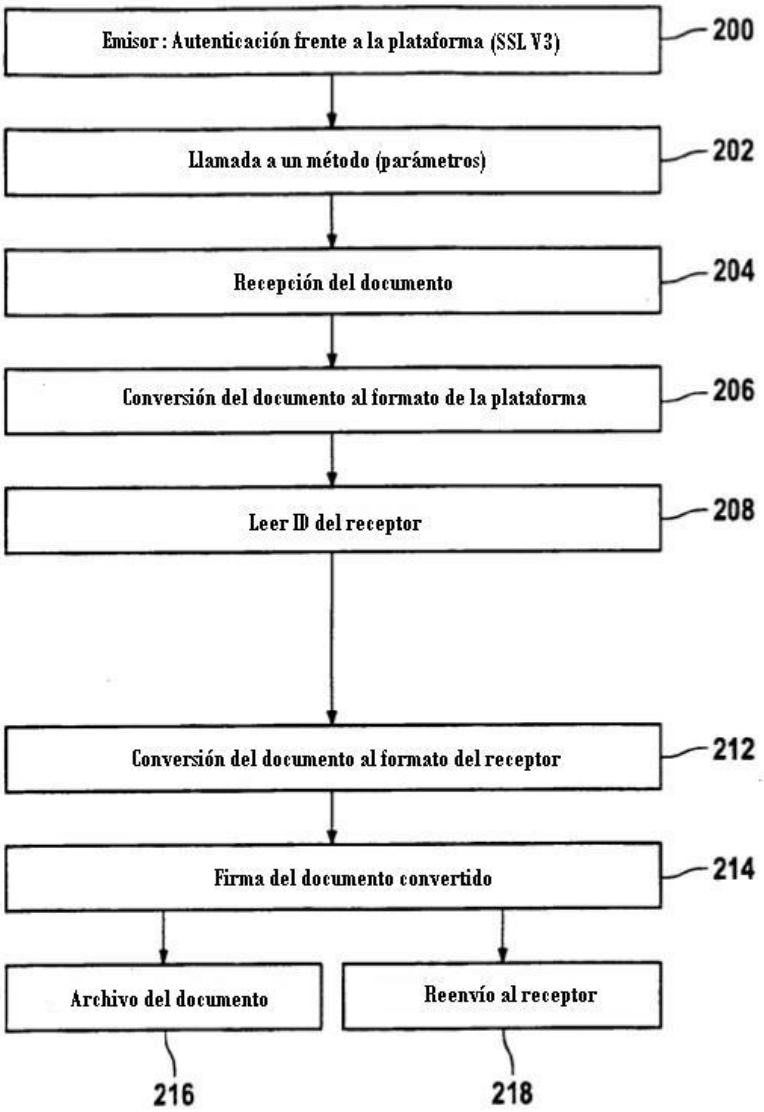

Emisor : Autenticación frente a la plataforma (SSL V3)
200
Llamada a un método (parámetros)
202
Recepción del documento
204
Conversión del documento al formato de la plataforma
206
Leer ID del receptor
208
Conversión del documento al formato del receptor
212
Firma del documento convertido
214
Archivo del documento
Reenvío al receptor
216
218

Fig. 3

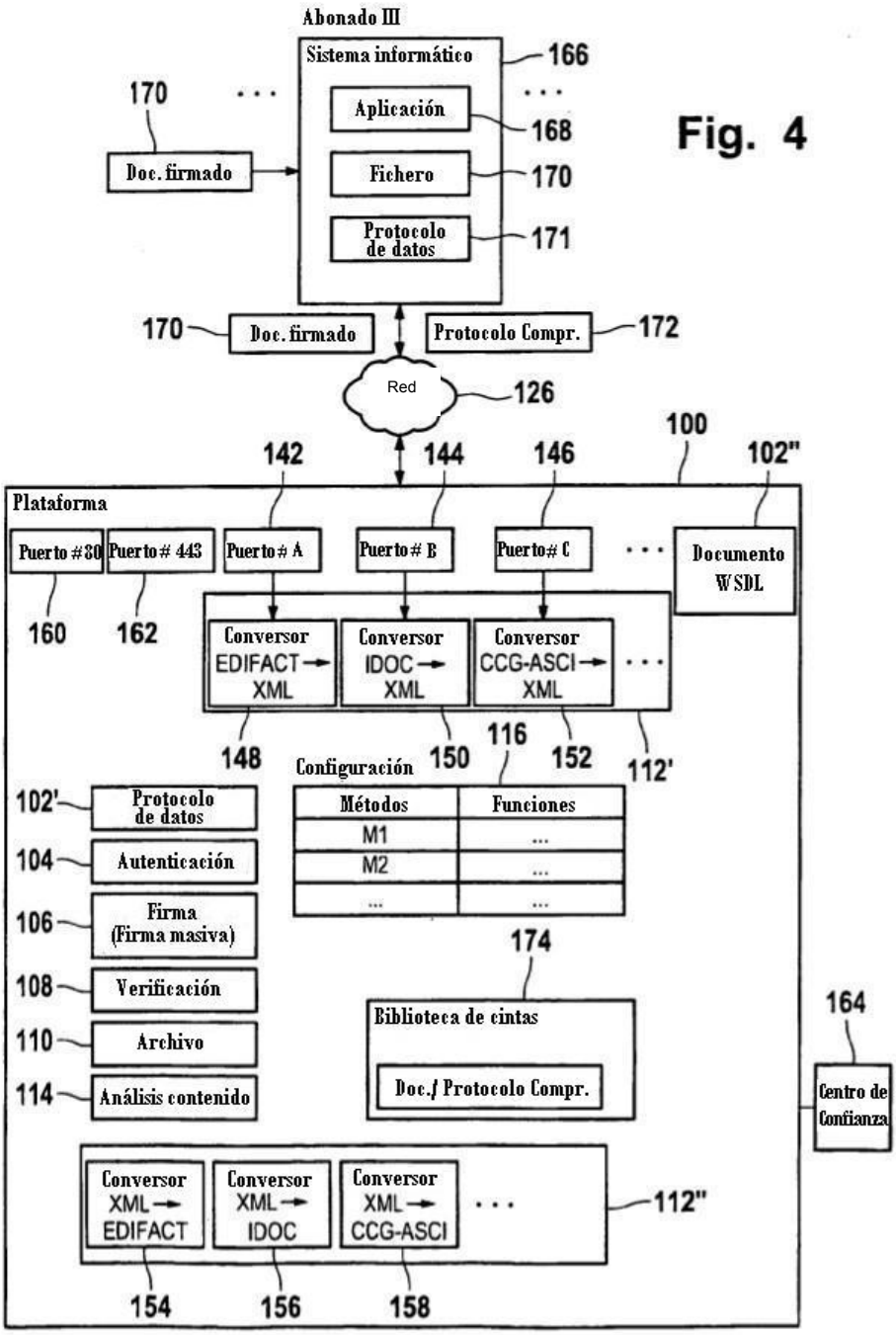

Abonado III
Sistema informático
166
170
Aplicación
168
Doc. firmado
Fichero
170
Protocolo de datos
171
170
Doc. firmado
Protocolo Compr.
172
Red
126
100
142
144
146
102"
Plataforma
Puerto #80
Puerto# 443
Puerto# A
Puerto# B
Puerto# C
Documento WSDL
160
162
Conversor EDIFACT → XML
Conversor IDOC → XML
Conversor CCG-ASCI → XML
148
150
116
152
112'
Configuración
Métodos
Funciones
M1
M2
102'
Protocolo de datos
104
Autenticación
106
Firma (Firma masiva)
108
Verificación
110
Archivo
114
Análisis contenido
174
Biblioteca de cintas
Doc./ Protocolo Compr.
164
Centro de Confianza
Conversor XML → EDIFACT
Conversor XML → IDOC
Conversor XML → CCG-ASCI
112"
154
156
158

Fig. 4

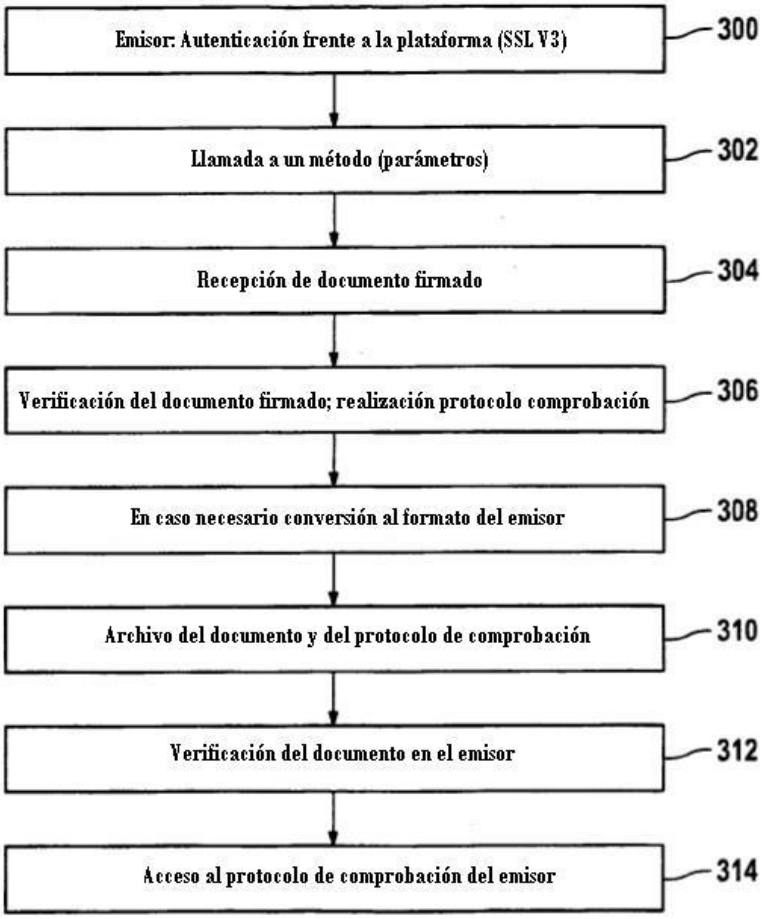

Emisor: Autenticación frente a la plataforma (SSL V3)
300
Llamada a un método (parámetros)
302
Recepción de documento firmado
304
Verificación del documento firmado; realización protocolo comprobación
306
En caso necesario conversión al formato del emisor
308
Archivo del documento y del protocolo de comprobación
310
Verificación del documento en el emisor
312
Acceso al protocolo de comprobación del emisor
314

Fig. 5

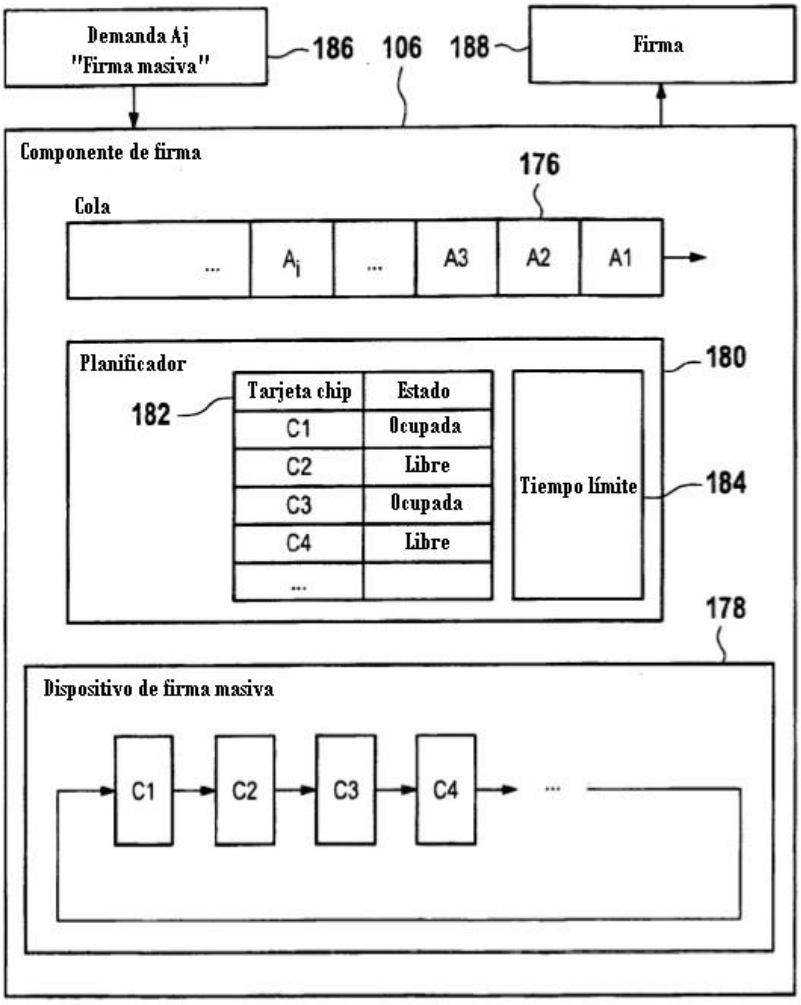

Demanda Aj
"Firma masiva"
186
106
188
Firma
Componente de firma
176
Cola
...
Ai
...
A3
A2
A1
Planificador
180
182
Tarjeta chip
Estado
C1
Ocupada
C2
Libre
C3
Ocupada
C4
Libre
...
Tiempo límite
184
178
Dispositivo de firma masiva
C1
C2
C3
C4
...

Fig. 6

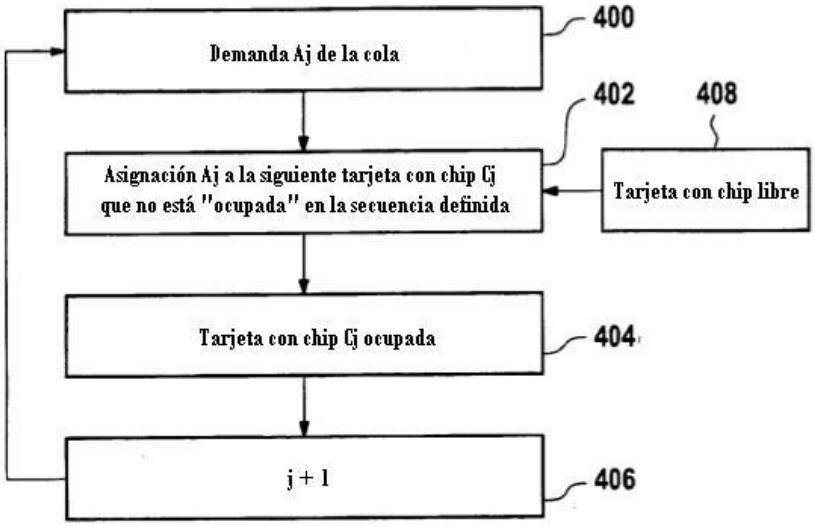

Demanda Aj de la cola
400
Asignación Aj a la siguiente tarjeta con chip Cj
que no está "ocupada" en la secuencia definida
402
408
Tarjeta con chip libre
Tarjeta con chip Cj ocupada
404
j + 1
406

Fig. 7