(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 704 150**

(51) Int. CI.:

G06Q 20/10 (2012.01)
H04L 29/06 (2006.01)
G06Q 20/20 (2012.01)
G06Q 20/36 (2012.01)
G06Q 40/00 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.06.2006 PCT/IB2006/001684**

(87) Fecha y número de publicación internacional: **28.12.2006 WO06136923**

(96) Fecha de presentación y número de la solicitud europea: **22.06.2006 E 06765574 (6)**

(97) Fecha y número de publicación de la concesión europea: **01.08.2018 EP 1894385**

(54) Título: **Método y sistema que utiliza un objeto portátil para proporcionar una extensión a un servidor**

(30) Prioridad:

24.06.2005 EP 05291370

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.03.2019

(73) Titular/es:

GEMALTO SA (100.0%)
6, rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es:

CASTILLO, LAURENT y
SIEGELIN, CHRISTOPH

(74) Agente/Representante:

CASANOVAS CASSÁ, Buenaventura

DESCRIPCIÓN

Método y sistema que utiliza un objeto portátil para proporcionar una extensión a un servidor

La presente invención se refiere al dominio de los servidores que ofrecen servicios a al menos un cliente, y más particularmente a servidores de Internet que ofrecen servicios en línea.

CAMPO TÉCNICO

Internet ofrece actualmente una amplia variedad de servicios y aplicaciones útiles. La mayoría usa el modelo cliente/servidor, en el que un cliente realiza peticiones a un servidor/es central/es. Puede haber muchas peticiones simultáneas de clientes, mientras que el servidor a menudo es una única máquina (un grupo de ordenadores como mucho).

El factor limitante en esos sistemas es a menudo las capacidades físicas del servidor: su ancho de banda disponible y su poder de computación. De hecho, la petición del cliente apenas llena el ancho de banda del cliente ni utiliza toda su potencia, mientras que la recopilación de todas las peticiones del cliente puede generar grandes cargas en la parte del servidor, ya sea de forma permanente o puntual, e incluso sobrecargar dicho servidor. Existen muchos casos en los que el servidor debe lidiar con una gran cantidad de conexiones simultáneamente.

Una forma de resolver este problema, desarrollado recientemente, es delegar parte de la computación al cliente (computación distribuida): los cálculos necesarios del servidor se reducen por la cantidad de éstos que se realizan por el lado del cliente. El ancho de banda puede reducirse utilizando un esquema de compresión o reduciendo la cantidad de datos a transferir (ya que parte son gestionados por el cliente). El almacenamiento del cliente también se puede usar para disminuir la cantidad de datos almacenados en el lado del servidor.

Sin embargo, otro problema principal surge cuando el servidor necesita ofrecer un servicio con un alto grado de seguridad y/o a prueba de manipulación. De hecho, en el modelo común de computación distribuida, el lado del cliente está lejos de ser confiable: puede ser comprometido por terceros a través de gusanos o virus o incluso por el propio cliente cuando éste tiene algún interés en engañar al servidor. Por lo tanto, no es posible utilizar el modelo de computación distribuida descrito anteriormente para servicios "seguros" y tenemos las restricciones comunes del modelo cliente/servidor bajo cargas elevadas. En los siguientes apartados usamos dos ejemplos de esos sistemas de carga elevada, que no limitan el alcance de la invención, que hacen frente a los problemas anteriores.

El primer ejemplo es la declaración en línea y el pago de impuestos. El servidor principal autentica al ciudadano y garantiza una fecha de declaración/pago. Es evidente que dicho servidor debe estar protegido tanto de terceros como del propio usuario. Por lo general, en la fecha de vencimiento el servidor hace frente a un elevado número de peticiones de manera simultánea, lo que en el mejor de los casos, genera un tiempo de procesamiento lento para cada petición.

El segundo ejemplo se refiere a los juegos en línea en modo multijugador masivos. En este ejemplo, el servidor debe resolver cada acción realizada por los jugadores y devolver los resultados. Es un proceso bastante ambicioso en términos de potencia computacional y ancho de banda. Para evitar las trampas, no se puede delegar la mayoría de esos cálculos en los ordenadores del cliente. En los últimos años, esos juegos se han desarrollado ampliamente y es corriente que un único servidor aloje a miles de jugadores todo el día.

La publicación de la solicitud de patente US 2002/0174071 A1 revela un método para cargar un programa de software en una tarjeta inteligente, en particular un applet.

Un objetivo de la presente invención es reducir la carga de conexión en el servidor.

Otro objetivo de la presente invención es ofrecer un servicio seguro y confiable.

SUMARIO DE LA INVENCIÓN

Esta invención se refiere a un método para extender un servidor conectado con al menos un cliente(s),
en el que se proporciona una extensión del servidor en el lado del cliente por medio de un objeto portátil SPO que se encuentra conectado a dicho cliente, comprendiendo dicho objeto portátil SPO medios de procesamiento y de almacenamiento de datos, que además comprende:

- una parte de la extensión adaptada para reducir la carga en el servidor mediante la realización de parte del procesamiento del servidor y que comprende una parte del software del servidor, una parte del almacenamiento del servidor y un esquema de compresión de datos,
- una parte confiable adaptada para garantizar que el servidor pueda confiar de forma segura en los datos provenientes de varios SPOs del lado de los clientes y que comprende partes de autenticación, personalización y registros de hora.

comprendiendo el método las etapas de:

- establecimiento de un enlace confiable, cifrado y una referencia de tiempo confiable gracias a una comunicación de las partes de autenticación y de registro de hora con el servidor;
- realización de al menos una de las operaciones del servidor de forma parcial o total por la parte de la extensión para gestionar al menos una solicitud del cliente y el almacenamiento local de la información del usuario relacionado, reportando de vuelta los resultados relevantes de la solicitud utilizando el esquema de compresión.

Esta invención también se refiere a un objeto portátil en el que se implementa dicho método.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Otros propósitos, características y ventajas de la invención aparecerán en la lectura de la descripción que sigue a continuación de la implementación del método de acuerdo con la invención y de un modo de realización de un objeto portátil diseñado para esta implementación, dado a título de ejemplo no limitativo, y haciendo referencia a los dibujos adjuntos en los que:

- la figura 1 es una vista esquemática de un ejemplo de realización de una unidad electrónica integrada en un objeto portátil tal como una tarjeta inteligente de acuerdo con la presente invención;
- la figura 2 se divide en dos partes que permiten comparar: a la izquierda, una vista esquemática de los diferentes pasos del proceso cliente/servidor conocido y, a la derecha, una vista esquemática de un modo de realización no limitativo de los diferentes pasos del método de acuerdo con la presente invención;
- la figura 3 es una vista esquemática de un modo de realización no limitativo de los componentes principales del objeto portátil de acuerdo con la presente invención de dos tipos, los "confiables" en gris y los de la "extensión" designados por flechas y su relación con el servidor y/o con el cliente;
- la figura 4 es una vista esquemática de un modo de realización no limitativo de las diferentes etapas del método de acuerdo la presente invención implementado por los componentes "confiables" ilustrados en la figura 3;
- la figura 5 es una vista esquemática de un modo de realización no limitativo de las diferentes etapas del método de acuerdo con la presente invención implementado por los componentes de la " extensión" ilustrados en la figura 3;
- la figura 6 es una vista esquemática de un ejemplo práctico de un uso del objeto portátil de acuerdo con la presente invención;
- la figura 7 es una vista esquemática de otro ejemplo práctico de un uso del objeto portátil de acuerdo con la presente invención.

MODO DE REALIZACIÓN IDEAL DE LA INVENCIÓN

El método de acuerdo con la presente invención pertenece al campo de los montajes electrónicos y por ejemplo al de los objetos portátiles tal como una tarjeta inteligente que comprende al menos medios de procesamiento tales como un procesador, medios de almacenamiento tales como una memoria y conectores capaces de conectar dicho objeto portátil a al menos un dispositivo portátil de aceptación de objetos con el que el objeto portátil puede trabajar o dialogar. En la realización descrita a continuación, el dispositivo portátil que acepta objetos es un cliente.

La tarjeta inteligente es un pequeño dispositivo de plástico que contiene uno o más circuitos integrados incorporados. Una tarjeta con circuito integrado puede ser, por ejemplo, una tarjeta de microprocesador.

Las tarjetas inteligentes se han desarrollado de tal manera que ahora ofrecen una gran potencia de computación asociada con un espacio de almacenamiento más grande (memorias flash y memorias externas). Recientemente, también ha incluido los mismos protocolos de comunicación que Internet y entradas/salidas físicas de alta velocidad (como USB, por ejemplo). En particular, tienen la capacidad de usar el ordenador host como un punto de acceso a Internet, de forma transparente para el host.

El método de acuerdo con la presente invención permite realizar una operación segura en un entorno inseguro comprendiendo al cliente mediante la utilización de dicho objeto portátil que constituye un entorno seguro. Así, utilizando un objeto portátil como una tarjeta inteligente, esas operaciones se procesan de forma segura. Además, al realizar operaciones previamente gestionadas por el servidor, el objeto portátil reduce la sobrecarga del servidor.

En una realización particular de la presente invención mostrada en la figura 1, el objeto portátil es una tarjeta inteligente con una unidad electrónica integrada 1: la unidad electrónica 1 comprende al menos un microprocesador CPU 3 con conexión bidireccional a través de un bus interno 5 a una memoria no volátil 7 de tipo ROM, EEPROM, Flash, FeRam o almacena al menos un programa para ser ejecutado, una memoria volátil 11 de tipo RAM y medios de entrada/salida I/O 13 para comunicarse con el exterior y de ahí en adelante con el servidor y el cliente. La unidad 1 puede comprender componentes adicionales no mostrados, conectados al bus interno. Este tipo de unidad se fabrica generalmente como un circuito electrónico monolítico integrado, o chip, que una vez que se protege

físicamente por cualquier medio conocido, puede ser ensamblado en la tarjeta de circuito integrado o similar para su uso en diversos campos, como el bancario y/o tarjetas de pago electrónico, radiotelefonía móvil, televisión de pago, salud y transporte...

El sistema de la presente invención también comprende un servidor conectado a al menos un cliente. El servidor ofrece información, servicios y funcionalidades o está a disposición. El cliente realiza peticiones al servidor para explotar esa información. El servidor y el cliente pueden tener numerosas formas posibles de realización. Comprenden al menos medios de procesamiento tales como un procesador, medios de almacenamiento tales como una memoria y conectores capaces de conectar dicho servidor y el cliente entre sí y con otro dispositivo tal como el citado objeto portátil para el cliente.

El principio del método de acuerdo con la presente invención es el siguiente.

El modelo cliente/servidor permite una distribución del procesamiento entre los clientes que solicitan al servidor la información requerida. En la presente invención, los clientes también piden a dicho objeto portátil obtener parte de esta información.

La presente invención es una extensión del modelo cliente/servidor que usa computación distribuida en objetos portátiles seguros para implementar "extensiones del servidor de confianza" en el lado del cliente.

La invención consiste en crear una extensión confiable del servidor con un Objeto Portátil Seguro (SPO), del lado del cliente. La mayoría de las veces, el cliente se comunicará con el SPO para gestionar sus peticiones, el SPO solo se pondrá en contacto con el servidor de vez en cuando (ver fig. 2 - Tráfico diseñado por el número (6) en parte respaldado por el tráfico entre el cliente (1) y la tarjeta (4). La extensión es tal que reduce tanto la CPU necesaria en el lado del servidor como el flujo de datos entre el cliente y el servidor.

La figura 2 compara el modelo tradicional cliente/servidor de la izquierda con el modelo mejorado según la presente invención a la derecha. En el modelo tradicional, los clientes ((1)) envían peticiones al servidor ((2)) y la cantidad total de peticiones genera una gran carga en los recursos del servidor ((5)). En el modelo mejorado, el servidor ((3)) se modifica ligeramente para comunicarse con el SPO ((4)) en casa del cliente. El SPO gestiona parte del trabajo del servidor de modo que la mayoría de las comunicaciones son locales entre el SPO y el ordenador del cliente. Los clientes también pueden comunicarse con el servidor para servicios genéricos o complejos, y el SPO tener que reportar información de vuelta al servidor, pero aun así la suma de todos los flujos de datos resulta menor que en el modelo anterior ((6)).

En la realización ilustrada, el SPO está conectado directamente al cliente. El cliente está conectado directamente al servidor. El SPO se conecta indirectamente al servidor a través del cliente y puede comunicarse directamente con el servidor a través de la capa de red como muestran las figuras 2 y 3.

La Figura 3 describe los componentes principales de la extensión SPO y sus interacciones con otros actores. En primer lugar, el SPO se puede usar en la red gracias a las nuevas tecnologías conocidas. Esta es la capa inferior básica de todas las comunicaciones entre el SPO, clientes y servidores.

El método de acuerdo con la presente invención comprende dos partes: la parte "confiable" (representada en la figura 3 en gris) y la parte de la " extensión" (designada en la figura 3 por flechas).

La parte "confiable" garantiza que el servidor puede confiar de forma segura en los datos de los diversos SPOs del lado de los clientes, y requiere las siguientes capacidades:

- Autentificación
- Personalización
- Registros de hora

Esas áreas grises permiten implementar un enlace de confianza con el SPO. Las partes de Autenticación y de Registro de hora se comunican con el servidor para establecer un enlace cifrado confiable y una referencia de tiempo confiable. La parte de Personalización es utilizada por el cliente para recuperar los datos personales del usuario, como si estuvieran almacenados en el servidor central. También facilita las fases de identificación e inicio de sesión con el servidor.

La parte de "extensión" reduce la carga en el servidor haciendo parte del trabajo del mismo y optimizando todo el proceso. Incluye:

- Parte del software del servidor
- Parte del almacenamiento del servidor
- Un esquema de compresión de datos

Las áreas blancas de la figura 3 implementan la extensión del servidor. Parte del software del servidor se delega en el SPO. Este software gestiona las peticiones del cliente (o algunas de ellas), y el almacenamiento local para la información relacionada con el usuario. El SPO usa un esquema de compresión con el servidor para reportar de vuelta los resultados relevantes de las peticiones, de modo que el ancho de banda se reduce aún más.

Para implementar la parte "confiable" (representada en la figura 4), el SPO utiliza sus capacidades de seguridad para implementar un protocolo de autenticación (por ejemplo, capacidades de cifrado). Primero, el SPO establece un enlace seguro a través de cualquier protocolo de autenticación y cifrado disponible ((1) - Figura 4). El cliente no puede entonces puntear este enlace, incluso si actúa como un proxy (evitando así las trampas del lado del usuario). Como la autenticación es realizada por el SPO, el usuario se libera de casi todos los procesos de autenticación con el servidor. Como se realiza una vez, la autenticación no consume demasiados recursos.

El SPO puede obtener opcionalmente una referencia de tiempo de un reloj del servidor ((2) - Figura 4). Esta referencia se puede usar para validar operaciones si se transmiten mucho después. El SPO intercambia registros de hora con el servidor, después de la autenticación, para obtener una fecha válida que puede usarse como prueba de la hora de las transacciones. Es una parte necesaria para los servicios que tienen una restricción de tiempo.

A continuación, el cliente puede recuperar datos personalizados del SPO, sin preguntar al servidor ((3) - Figura 4). El SPO puede contener información previamente personalizada sobre el usuario, lo que agilizará las entradas del usuario y liberará al servidor de esa etapa necesaria. Estos datos tienen el mismo grado de confiabilidad que si provinieran del servidor. Esa etapa puede proteger contra terceros en los ataques intermedios.

El SPO y el cliente entran entonces en el modo de ejecución normal (Figura 4).

Por último, el SPO puede reportar datos de vuelta, encriptados y con registros de hora ((4)). El servidor puede considerar esto como si hiciera él mismo la transacción.

La distribución del SPO está garantizada por los operadores del servicio, que pueden entonces confiar en la etapa de personalización de SPO.

Por la parte de la " extensión" (Fig. 5), el software del servidor se rediseña para que parte de su trabajo se realice en el SPO. Con mucha frecuencia, la petición de un cliente es fácil de gestionar, solo la cantidad acumulada de peticiones crea una sobrecarga. El SPO puede gestionar fácilmente peticiones simples de un solo cliente y reportar únicamente al servidor los resultados de un lote completo de peticiones. En otros casos, el SPO puede gestionar cálculos intermedios para una petición y ayudar a simplificar toda petición en el lado del servidor.

El SPO también puede aplicar un esquema de compresión en sus datos, de modo que el ancho de banda necesario entre el cliente del SPO y el servidor se reduzca aún más. Todos los datos y resultados de la petición, así como la información personalizada pueden almacenarse en el SPO, reduciendo así la cantidad de almacenamiento necesaria en el servidor. El servidor puede también utilizar el SPO como una red de almacenamiento genérica distribuida.

Un ejemplo de implementación del mecanismo de extensión del servidor se describe en relación con la figura 5. El software del servidor es dividido de modo que parte de él resida en el SPO. La mayoría de las veces, el cliente pedirá al SPO peticiones ((1)) o información ((2)). El software del cliente se ejecuta en un bucle ((3)), solicitando peticiones hasta la finalización. Periódicamente (o justo al final), el SPO puede tener que reportar de vuelta y/o sincronizar datos con el servidor ((4)). Esta etapa puede usar compresión para liberar el ancho de banda y los registros de hora para ayudar en el proceso de sincronización.

Las ventajas ofrecidas por dicho método y dicho sistema son numerosas. El método y el sistema según la presente invención reducen la carga de conexión en el servidor, la potencia de cálculo necesaria e incluso el espacio de almacenamiento. Los beneficios son una mejor calidad de servicio o un incremento del número de usuarios simultáneos.

Dos ejemplos de aplicación de la presente invención se describen a continuación en detalle.
La primera aplicación es una declaración de impuestos en línea (Fig. 6). Las características en este sistema son:

Se necesita una sólida seguridad para protegerse de los ataques de terceros.
Alta carga en un momento determinado, con importantes consecuencias.

En la presente invención, el gobierno distribuye el SPO con la declaración en papel común (con solo un pequeño coste adicional) y toda la información personalizada del contribuyente (dirección, estado civil, etc.).

Cuando el contribuyente desea realizar la declaración en línea, simplemente conecta el SPO a su ordenador (y, por lo tanto, con Internet). El SPO se autentica a sí mismo y al usuario al servidor oficial del gobierno (paso (1) en la figura 6), ayudado por los datos personales almacenados en el SPO. Obtiene entonces un sello de fecha o registro

de hora del servidor para la declaración (paso (2) en la figura 6). Ese es el único paso necesario entre el cliente/SPO y el servidor (muchos menos que en el modelo tradicional). Todos los pasos siguientes (representados por el paso (3) en la figura 6) de una declaración (cumplimentación de formularios, obtención de ayuda y cálculo de la cantidad estimada del impuesto, por ejemplo) son llevados a cabo entre el ordenador del cliente y el SPO, que contiene los formularios requeridos, las páginas y las fórmulas de cálculo. El cliente puede usar datos personales almacenados en el SPO, para obtener formularios parcialmente cumplimentados (para la declaración), herramientas de ayuda y cálculo, o similares. En el último paso, presentar la declaración (paso 4 en la figura 6), el usuario tiene entonces dos opciones: o se conecta de nuevo al servidor y reporta la declaración presentada al servidor en un archivo comprimido y encriptado, o simplemente devuelve el SPO a la administración local, donde el registro de hora almacenada servirá como prueba de que la declaración fue presentada dentro de plazo.

La segunda aplicación lidia con juegos masivos multijugador. En los sistemas conocidos, el servidor mantiene un gran estado mundial virtual en la memoria, incluidos los personajes de los jugadores. Los jugadores pueden interactuar con el mundo y entre ellos. Las interacciones de los jugadores con el mundo deben ser resueltas por el servidor para evitar trampas. El servidor está conectado en todo momento a miles de jugadores, cuyo número solo está limitado por la capacidad del servidor (cuantos más jugadores haya, más interesante resulta). Las características son entonces:

- Se necesita una sólida seguridad para protegerse de los ataques de los usuarios.
- Alta carga durante todo el día, lo que limita el alcance del juego.

En la presente invención (ilustrada en la figura 7), el SPO se distribuye con el CD del juego, a través del dispositivo de juego habitual. El SPO sirve como autenticación de un propietario legítimo (incluido incluso el pago de las tarifas del juego) y como almacenamiento de la información del jugador (personajes, puntos, etc.): acceso más fácil para el jugador y menos almacenamiento para el servidor. Sin embargo, el principal punto de la invención es que el par SPO-servidor está diseñado para que el SPO realice una parte del trabajo del servidor.

Por ejemplo, una solución simple es que el SPO pueda gestionar cada acción que afecte solo al jugador mismo (no se necesita sincronización entre el SPO y el servidor). En escenarios más complejos, el servidor puede usar el registro de hora en los SPO (fechas confiables) para sincronizar acciones conflictivas. El SPO puede conectarse al servidor del juego de forma limitada y solo para acciones conflictivas o para "resúmenes" periódicos, lo que reducirá drásticamente el ancho de banda necesario.

La Figura 7 describe el modelo de ejecución en los juegos multijugador, que es un poco más complicado. De hecho, el SPO no puede hacer todo el trabajo del servidor. Algunas acciones simples o no conflictivas realizadas por el jugador son resueltas enteramente por la tarjeta (SPO) y contestadas inmediatamente ((1) y (1)'). El SPO debe reportar de vuelta, de tanto en tanto, al servidor (con fines de copia de seguridad o seguimiento), resumiendo todos estos resultados de acciones ((4) y luego (5)). Algunas acciones conflictivas requieren tratamiento por parte del servidor central. Éstas son tratadas previamente por el SPO para liberar al servidor tanto como sea posible y luego son reenviadas al servidor ((2) y luego (3)). Los resultados de las acciones se envían de vuelta a través del SPO ((3)' y luego (2)').

REIVINDICACIONES

1. Método para extender un servidor conectado con al menos un cliente, en el que se proporciona una extensión del servidor en el lado del cliente por medio de un objeto portátil SPO (1) que está conectado a dicho cliente, comprendiendo dicho objeto portátil SPO (1) medios de procesamiento y almacenamiento de datos, y que además comprende:

- una parte de extensión adaptada para reducir la carga en el servidor mediante la realización de parte del procesamiento del servidor y que incluye una parte del software del servidor, una parte del almacenamiento de datos y un esquema de compresión de datos,
- una parte confiable adaptada para garantizar que el servidor puede confiar de forma segura en los datos provenientes de varios SPOs del lado de los clientes y que comprende partes para la autenticación, personalización y registro de hora;

comprendiendo el método las etapas de :

- establecimiento de un enlace confiable, cifrado y una referencia de tiempo confiable gracias a una comunicación de las partes de autenticación y de registro de hora con el servidor;
- realización de al menos una de las operaciones del servidor de forma parcial o total por la parte de la extensión para gestionar al menos una solicitud del cliente y el almacenamiento local de la información del usuario relacionado,
- reportando de vuelta los resultados relevantes de la solicitud utilizando el esquema de compresión.

2. Método según la reivindicación 1, **caracterizado porque** consiste en proporcionar fiabilidad para la parte confiable del objeto portátil por medio del entorno seguro y las operaciones criptográficas que ofrece dicho objeto portátil.

3. Método según una de las reivindicaciones 1 a 2, **caracterizado porque** consiste en gestionar al menos una de las solicitudes enviadas desde dicho cliente a dicho servidor por medio de dicho objeto portátil e informar los resultados de dicha solicitud o de un conjunto de solicitudes a dicho servidor.

4. Método según una de las reivindicaciones 1 a 3, **caracterizado porque** consiste en establecer un enlace seguro con dicho objeto portátil a través de un protocolo de autenticación y cifrado.

5. Método según una de las reivindicaciones 1 a 4, **caracterizado porque** consiste en intercambiar, entre dicho objeto portátil y dicho servidor, una referencia de tiempo para ser usada como una prueba de al menos una operación.

6. Método según una de las reivindicaciones 1 a 5, **caracterizado porque** consiste en proporcionar medios de compresión/descompresión en dicho objeto portátil que permite la compresión de datos a transferir desde y/o a dicho objeto portátil.

7. Método según una de las reivindicaciones 1 a 6, **caracterizado porque** consiste en almacenar parte de la información utilizada en la relación cliente/servidor en dicho objeto portátil.

8. Método para realizar la declaración fiscal en línea que comprende las etapas del método según cualquiera de las reivindicaciones 1 a 7, en el que dicho objeto portátil recupera un registro de hora válido del servidor como prueba de la fecha de declaración, donde un declarante es autenticado por dicho objeto portátil y donde todas o parte de las operaciones relacionadas con el rellenado del formulario de declaración de impuestos son gestionadas por dicho objeto portátil.

9. Método para jugar en línea que comprende las etapas del método según cualquiera de las reivindicaciones 1 a 7, donde algunas de las acciones realizadas por el jugador son resueltas de forma o total por dicho objeto portátil.

10. Un objeto portátil SPO (1) que comprende medios de procesamiento y almacenamiento de datos destinados a ser conectados a un cliente, estando dicho cliente conectado a un servidor, **caracterizado porque** dicho SPO (1) comprende:

- una parte de extensión adaptada para reducir la carga en el servidor mediante la realización de parte del procesamiento del servidor y que incluye una parte del software del servidor, una parte del almacenamiento de datos y un esquema de compresión de datos,
- una parte confiable adaptada para garantizar que el servidor puede confiar de forma segura en los datos provenientes del SPO del lado de los clientes y que comprende partes para la autenticación, personalización y registro de hora;

comprendiendo el método las etapas de :

- establecimiento de un enlace confiable, cifrado y una referencia de tiempo confiable gracias a una comunicación de las partes de autenticación y de registro de hora con el servidor;
- realización de al menos una de las operaciones del servidor de forma parcial o total por la parte de la extensión para gestionar al menos una solicitud del cliente y el almacenamiento local de la información del usuario relacionado,
- reportando de vuelta al servidor los resultados relevantes de la solicitud utilizando el esquema de compresión.

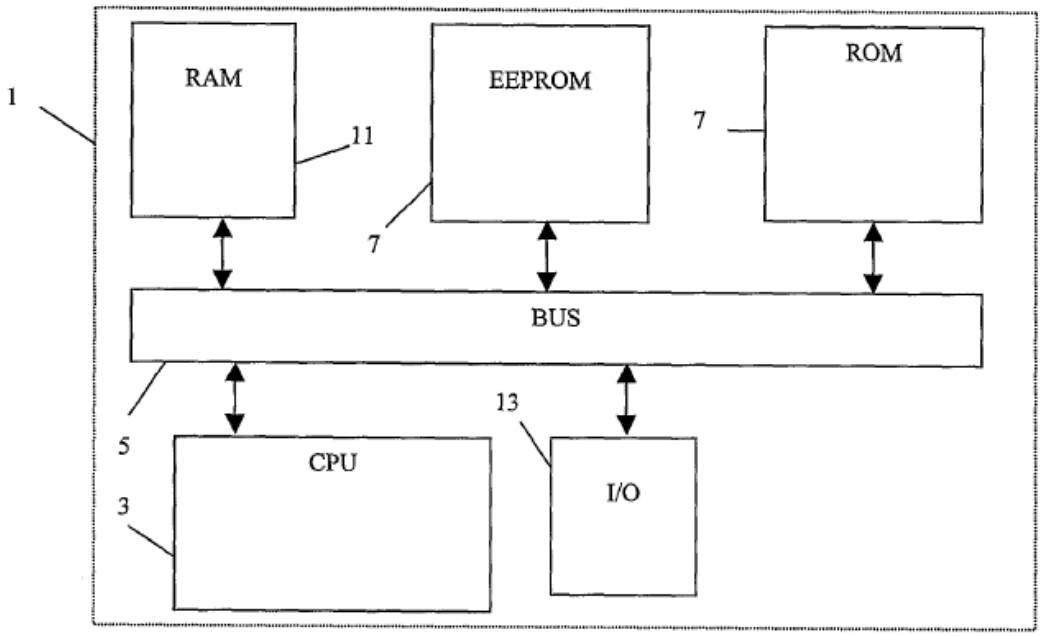
1
RAM
11
EEPROM
7
ROM
7
BUS
5
13
CPU
I/O
3

FIG.1

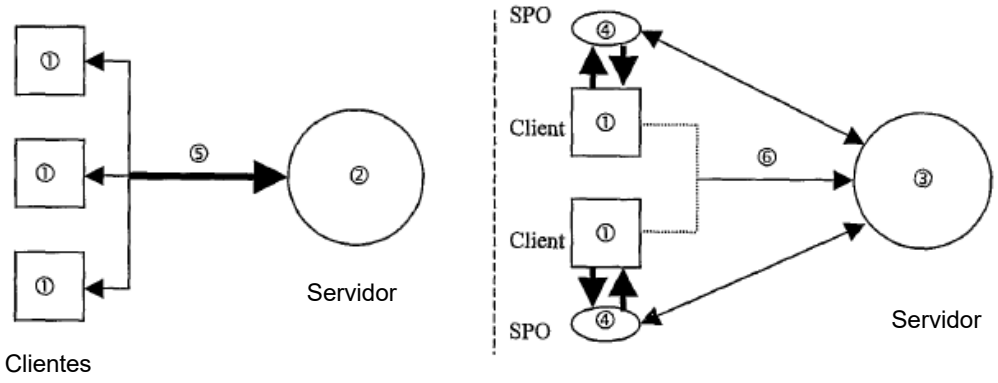
①
①
①
⑤
②
Servidor
Clientes
SPO
④
Client
①
⑥
③
Client
①
SPO
④
Servidor

FIG.2

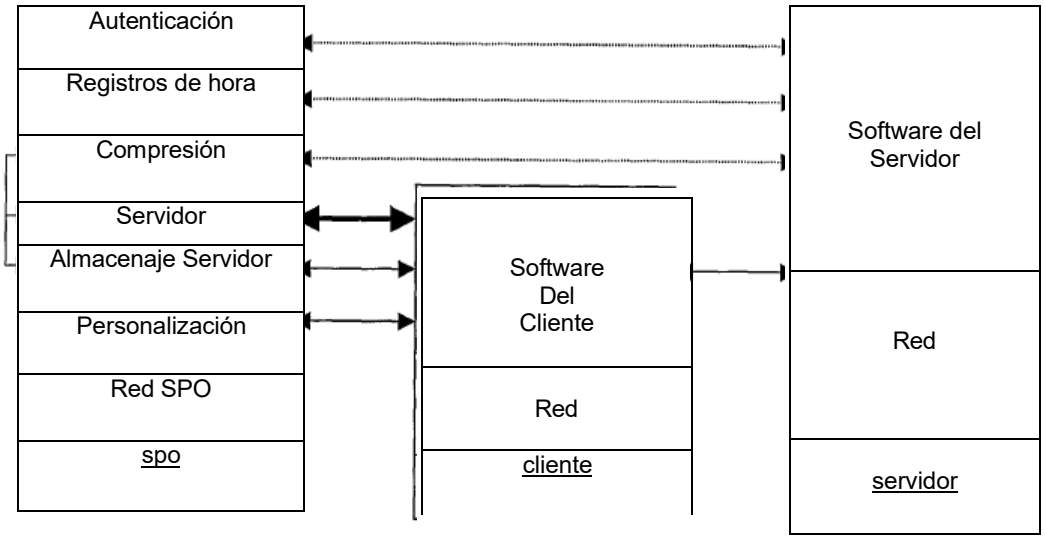
Autenticación
Registros de hora
Compresión
Servidor
Almacenaje Servidor
Personalización
Red SPO
spo
Software
Del
Cliente
Red
cliente
Software del
Servidor
Red
servidor

FIG.3

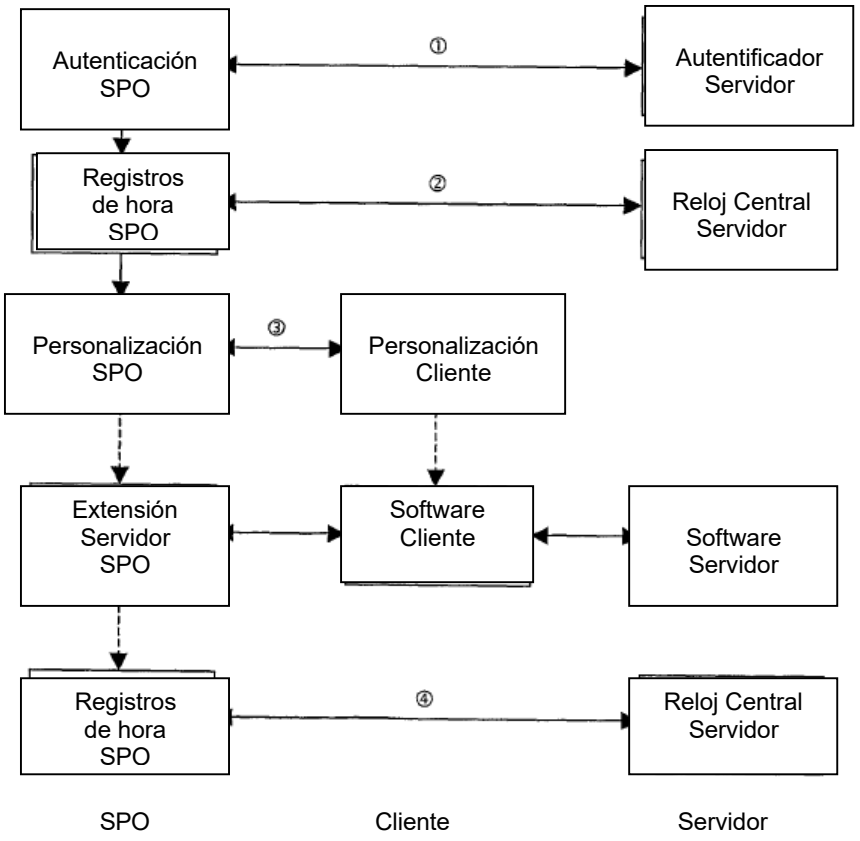
Autenticación
SPO
①
Autentificador
Servidor
Registros
de hora
SPO
②
Reloj Central
Servidor
Personalización
SPO
③
Personalización
Cliente
Extensión
Servidor
SPO
Software
Cliente
Software
Servidor
Registros
de hora
SPO
④
Reloj Central
Servidor
SPO
Cliente
Servidor

FIG.4

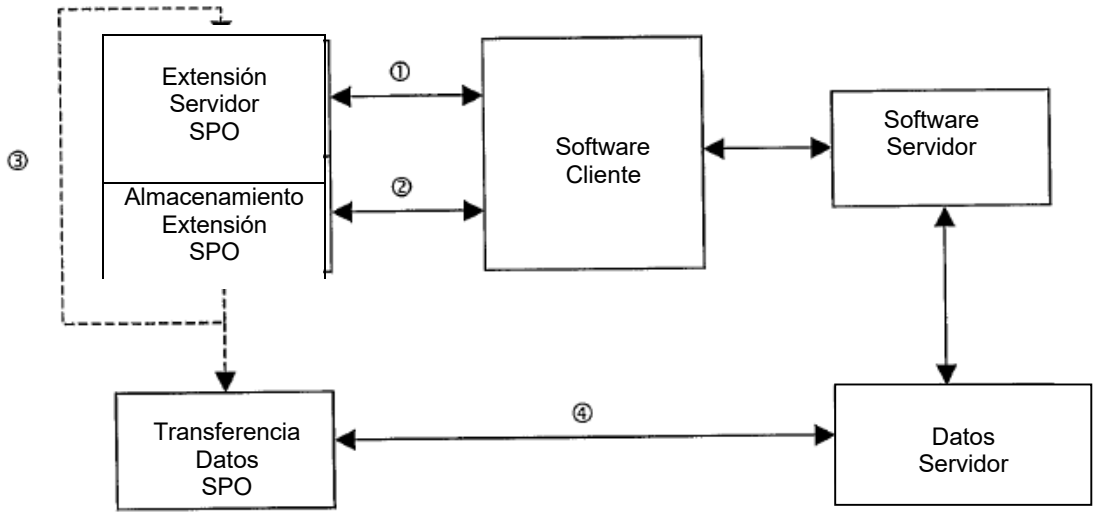
Extensión Servidor SPO
Almacenamiento Extensión SPO
Software Cliente
Software Servidor
Transferencia Datos SPO
Datos Servidor
①
②
③
④
SPO
Cliente
Servidor

FIG.5

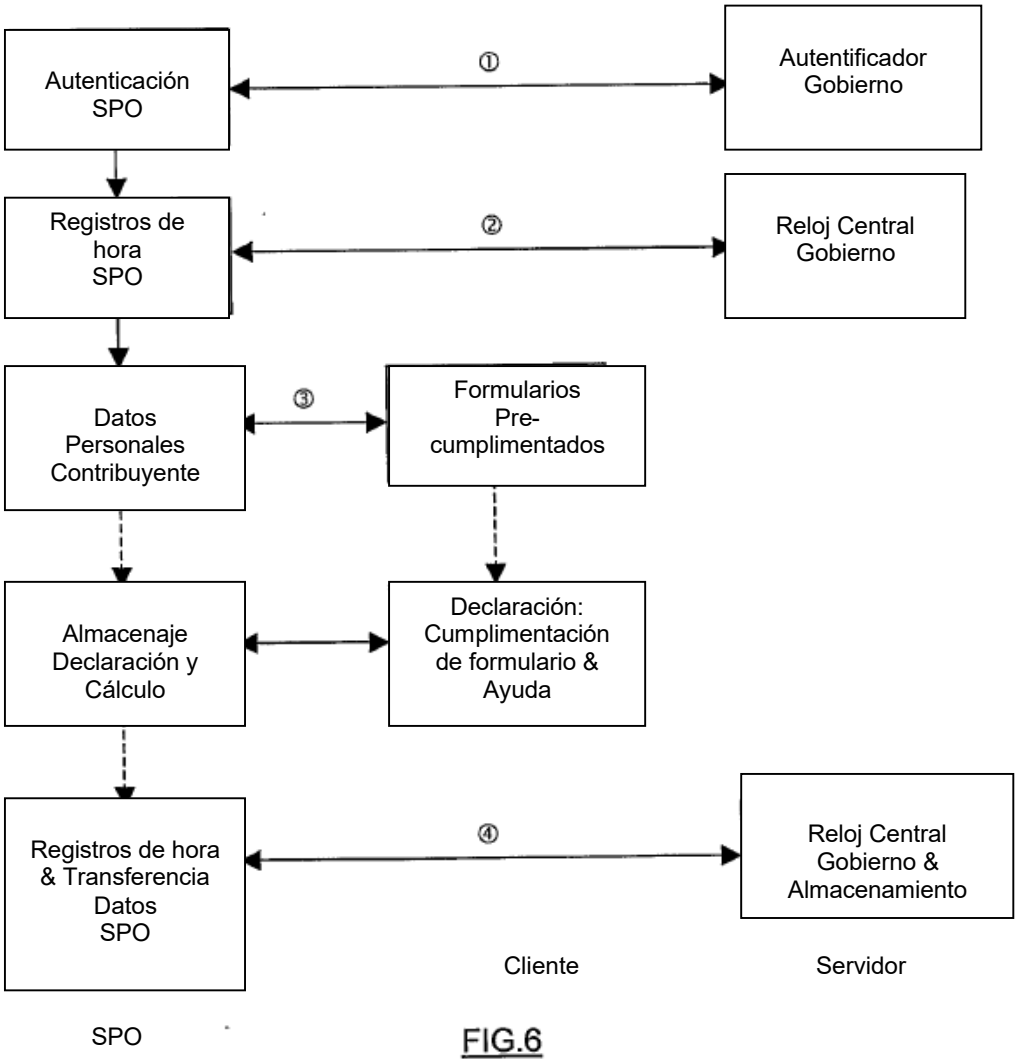
Autenticación SPO
Autentificador Gobierno
Registros de hora SPO
Reloj Central Gobierno
Datos Personales Contribuyente
Formularios Pre-cumplimentados
Almacenaje Declaración y Cálculo
Declaración: Cumplimentación de formulario & Ayuda
Registros de hora & Transferencia Datos SPO
Reloj Central Gobierno & Almacenamiento
①
②
③
④
Cliente
Servidor
SPO

FIG.6

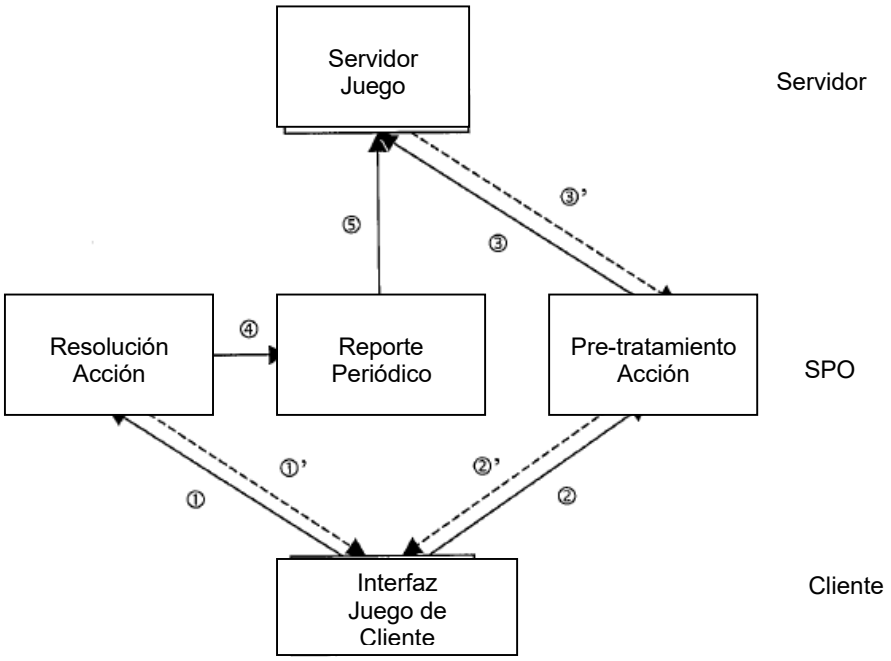
Servidor Juego
Servidor
③'
⑤
③
Resolución Acción
④
Reporte Periódico
Pre-tratamiento Acción
SPO
①'
②'
①
②
Interfaz Juego de Cliente
Cliente

FIG.7