(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 310 321**

(51) Int. Cl.:
G06F 21/00 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05250968 .4**
(96) Fecha de presentación : **21.02.2005**
(97) Número de publicación de la solicitud: **1628187**
(97) Fecha de publicación de la solicitud: **22.02.2006**

(54) Título: **Sistema y procedimiento para asegurar la transmisión continua de datos mediante una tarjeta inteligente virtual.**

(30) Prioridad: **01.10.2004 US 957081**

(45) Fecha de publicación de la mención BOPI:
01.01.2009

(45) Fecha de la publicación del folleto de la patente:
01.01.2009

(73) Titular/es: **Widevine Technologies, Inc.**
901 Fifth Avenue, Suite 3400
Seattle, Washington 98164, US

(72) Inventor/es: **Morten, Glenn A. y**
Baker, Brian

(74) Agente: **Curell Suñol, Marcelino**

DESCRIPCIÓN

Sistema y procedimiento para asegurar la transmisión continua de datos mediante una tarjeta inteligente virtual.

Campo técnico de la invención

La presente invención dispone un procedimiento para encriptar un flujo de datos con el fin de asegurar el flujo de datos para un único visionado y para proteger los derechos de reproducción del flujo de datos. Específicamente, la invención dispone un procedimiento para proteger la transmisión continua ("streaming") de productos multimedia, de entretenimiento y comunicaciones en una transmisión de tipo internet. La invención dispone asimismo una tarjeta inteligente virtual dentro de un sistema cliente que interactúa con un componente de un servidor de transmisión continua para llevar a cabo el procedimiento según la invención.

Antecedentes de la invención

Internet ofrece otros medios de comunicación mediante los cuales pueden transferirse datos desde un servidor a un cliente. El cliente es responsable de la visualización de los datos transferidos, preferiblemente datos multimedia transferidos, al usuario. El servidor es el responsable de la entrega del flujo de datos al cliente. Las soluciones Real Networks y Microsoft envían el flujo de datos a través de UPD (un protocolo de internet sin conexión) junto con otra conexión entre el cliente y el servidor que controla la transmisión de los datos transferidos. El elemento de conexión de control funciona para detener sobrecargas de la memoria intermedia y puede ajustar la transmisión del flujo para compensar latencias de ancho de banda. No obstante, un problema que plantea esta disposición es que los datos transferidos al cliente desde el servidor no están protegidos y son accesibles a cualquiera en la red. Por lo tanto, en la técnica existe una necesidad de mejor protección contra intercepciones a través de un red de cobertura amplia, como por ejemplo internet. Específicamente, la necesidad se refiere a proporcionar una capacidad de protección contra las intercepciones inadecuadas y contra la capacidad de copiar datos transferidos de manera continua a través de internet. Actualmente no existe ningún mecanismo de protección para proteger los datos registrados.

Una vez que los datos han sido liberados por el servidor y recibidos por el usuario, o interceptados antes de ser recibidos por el usuario, no hay modo de restringir la retransmisión de tales datos después de haber sido liberados en la red. Aunque el flujo de datos esté registrado, no existen medios para proteger o hacer cumplir los derechos registrados de los datos transferidos. La entidad propietaria del registro que transfiere este contenido asume que no existe control de lo que ocurre con dicho contenido una vez liberado. Por lo tanto, existe una necesidad en la técnica de disponer medios para proteger los contenidos con derechos registrados una vez que dichos contenidos son transferidos por la red. La presente invención se propone responder a ambas necesidades.

Una solución consiste en encriptar los datos que se envían desde el servidor al cliente. Esto puede realizarse utilizando tecnología existente, por ejemplo combinando los socket HTTP seguro SSL con un paquete de software de transmisión continua, por ejemplo Quicktime. Lamentablemente, el Quicktime no presenta una opción de vista en pantalla completa. Por lo tanto, existe una necesidad en la técnica de desarrollar un procedimiento mejor para la transferencia de datos de vídeo.

El documento US 2004/0117500 da a conocer un procedimiento de suministro de datos por transmisión continua en el cual un cliente envía un ticket de autorización a un servidor de transmisión continua para se comprobado para validar una solicitud de datos por transmisión continua. Si el ticket se considera válido, el servidor de transmisión continua encripta los datos y los envía al cliente. El cliente puede desencriptar los datos recibidos, por ejemplo utilizando una clave secreta contenida en un módulo de identidad del cliente.

Sumario de la invención

La presente invención dispone una arquitectura de dispositivo cliente particular que permite el control de flujo de datos de transmisión continua.

En un primer aspecto, la presente invención dispone un sistema para comunicar un flujo de datos a través de una red que comprende un dispositivo cliente configurado para realizar acciones, incluyendo permitir una solicitud de flujo de datos; un servidor de transmisión continua configurado para ejecutar acciones, incluyendo la validación de un testigo para un flujo de datos solicitado; y una tarjeta inteligente virtual acoplada al dispositivo cliente, estando configurada la tarjeta inteligente para llevar a cabo acciones, las cuales comprenden: negociación del testigo con el servidor de transmisión continua; almacenamiento del testigo obtenido como respuesta a la negociación en un módulo de almacenamiento de testigos (7100) situado en el interior de la tarjeta inteligente (7004); envío del testigo junto con el flujo de datos solicitado; recepción del flujo de datos solicitado, hallándose el flujo de datos solicitado encriptado; y provisión de una métrica de control de flujo asociada con el flujo de datos; estando configurado el servidor de transmisión continua para efectuar acciones adicionales en el caso de que el testigo sea válido para el flujo de datos solicitado, comprendiendo dichas acciones adicionales la transmisión del flujo de datos encriptado a la tarjeta inteligente virtual y utilización de la métrica de control de flujo de la tarjeta inteligente, en parte para controlar el flujo de datos encriptados a través de la red para mantener sustancialmente llena una memoria intermedia asociada con la tarjeta inteligente virtual, para que el flujo de datos pueda recibirse a la velocidad a la cual el dispositivo cliente utiliza los datos.

En un segundo aspecto, la presente invención dispone una señal de datos modulada para gestionar un flujo de datos a través de una red, comprendiendo la señal de datos modulada instrucciones dispuestas para efectuar acciones que comprenden: solicitud del flujo de datos por un cliente que dispone de una tarjeta inteligente virtual; negociación mediante la tarjeta inteligente virtual (7004) con un servidor para obtener un testigo asociado con el flujo de datos solicitado; almacenamiento del testigo obtenido como respuesta a la negociación en el módulo de almacenamiento de testigos (7100) dentro de la tarjeta inteligente virtual (7004); facilitación de la determinación de la validez del testigo para el flujo de datos solicitado; y, si el testigo es válido para el flujo de datos solicitado, facilitación de la negociación de una clave de encriptación con la tarjeta inteligente virtual; facilitación de la encriptación del flujo de datos cuando el flujo de datos se transmite al dispositivo cliente, efectuándose la encriptación del flujo de datos utilizando la clave de encriptación negociada; provisión por la tarjeta inteligente virtual de una métrica de control de flujo asociada con el flujo de datos encriptado; y control, mediante el servidor, de la velocidad de flujo del flujo de datos encriptado, a través de la red hasta el cliente, utilizando el servidor para ello la métrica de control de flujo, en parte para controlar la velocidad de flujo del flujo de datos encriptado de modo que la memoria intermedia del cliente se mantenga sustancialmente llena, con el fin de que el flujo de datos pueda ser recibido a la velocidad a la que el cliente utiliza los datos.

En un tercer aspecto de la presente invención, se dispone un procedimiento para comunicar un flujo de datos a través de una red que comprende las etapas siguientes solicitud del flujo de datos; utilización de un testigo negociado asociado con el flujo de datos solicitado para permitir la validación de la solicitud del flujo de datos; si la solicitud es válida, recepción del flujo de datos procedente de un servidor; incluyendo además el procedimiento las etapas siguientes: negociación con el servidor, mediante una tarjeta inteligente virtual acoplada al dispositivo cliente, del testigo asociado con el flujo de datos solicitado; almacenamiento en un módulo de almacenamiento de testigos (7100), situado en el interior de la tarjeta inteligente virtual (7004), del testigo obtenido como respuesta a la negociación; y suministro al servidor, por la tarjeta inteligente virtual, de una métrica que el servidor puede utilizar, en parte, para controlar la velocidad de flujo del flujo de datos, con el fin de mantener sustancialmente llena la memoria intermedia del cliente para que el flujo de datos pueda recibirse a la velocidad a la cual el dispositivo cliente utiliza los datos.

Breve descripción de los dibujos

La figura 1 representa un esquema del componente del cliente autorizado para recibir y visualizar un flujo de datos encriptado. El componente del cliente comprende un módulo de almacenamiento de testigos 100, un módulo de protocolo de control de flujo 120 y un módulo de desencriptación 160.

La figura 2 representa un esquema del componente servidor de transmisión continua que presenta por lo menos un módulo de encriptación 220 y un módulo de conexión de control del cliente para la negociación de claves y la verificación de testigos 200.

La figura 3 representa a un esquema de los componentes del servidor de transacciones que presenta un módulo de creación de testigos 330 y un módulo de verificación de usuario 310.

La figura 4 representa un esquema de diversos escenarios de cliente que muestran la necesidad de un testigo para abrir (desencriptar) un flujo de datos para su visualización.

La figura 5 representa un esquema del proceso para que el servidor de transmisión continua muestre la recepción de un testigo de cliente que provoca una negociación de claves de encriptación para permitir visualizar y recibir un flujo de datos.

La figura 6 representa un esquema del proceso del servidor de transacciones que dispone la apertura de cuentas de cliente y la creación de testigos.

La figura 7 representa una forma de realización de una tarjeta inteligente virtual (VSC) en el interior de un dispositivo cliente configurado para interactuar operativamente con un servidor de transacciones para gestionar un flujo de datos, según la presente invención.

Descripción detallada de la forma de realización preferida

La presente invención proporciona un procedimiento para encriptar un flujo de datos, por ejemplo comunicaciones y entretenimiento multimedia, a través de internet. El flujo de datos encriptado permitirá la transferencia de materiales con derechos registrados y las comunicaciones multimedia (por ejemplo reuniones de analistas, televisión interactiva, películas) sobre una base segura de pay-per-view y similares. El flujo de datos no puede almacenarse en el dispositivo del cliente para volverlo a reproducir ni puede ser retransmitido. No obstante, un cliente puede ver un flujo de datos tantas veces como desee en un marco de tiempo específico.

Un protocolo de encriptación dispone, por ejemplo, un algoritmo de encriptación de una clave de 192 bits (por ejemplo Triple DES), un protocolo de paquetes UDP, un protocolo de transmisión de paquetes RTSP (rfc 2326), un protocolo de control de transmisiones de paquetes RTP (rfc 1889) y compresión de almacenamiento de vídeo MPEGI. No obstante, el ejemplo anteriormente mencionado de un protocolo de encriptación preferido cambiará cuando estas

técnicas se perfeccionen con el tiempo. Por ejemplo, una forma de realización puede utilizar el Advanced Encryption Standard (AES) o un algoritmo de encriptación similar.

Una ventaja del procedimiento según la invención que utiliza el servidor de transmisión continua y el servidor de transacciones según la invención es que el cliente no necesita realmente disponer de un dispositivo completamente optimizado. Normalmente el cliente se ejecuta en cualquier dispositivo en cualquier momento. El cliente puede estar configurado para reproducir, por ejemplo vídeo a 320x240 30 fps y audio back sin latencia. Esto permite un flujo de datos de aproximadamente 250 - 300 kps, una memoria intermedia de datos grande (de por lo menos varios megabytes) y un procesador Pentium II 350 MHz o superior con Windows 98 o Windows NT. No obstante, el sistema cliente no está tan restringido y puede utilizarse virtualmente cualquier configuración de sistema cliente. Por ejemplo, el sistema cliente puede incluir un Set Top Box, capacidad de televisión interactiva y similares.

El servidor, por ejemplo, puede ser un servicio Windows NT multiproceso (threadpool) completamente optimizado. A diferencia de un servidor HTTP, esto permite guardar sesiones con clientes en la memoria temporal y el servidor necesitará mantener el estado respecto a todos los clientes.

Definiciones

Los siguientes términos se utilizan con los significados definidos a continuación. El cliente o sistema cliente se refiere al ordenador al cual se está enviando el flujo de datos. El usuario se refiere a la persona que ejecuta las instrucciones en el cliente.

Módulo significa un conjunto de código compilado diseñado para efectuar una función específica, o un conjunto de funciones.

URI (identificador universal de recursos) representa un identificador asociado con una ubicación del flujo en el servidor.

Testigo se refiere a una pieza de información binaria que comprende los permisos de los que dispone el usuario para un flujo de datos específico.

Autentificación se refiere a proporcionar un nivel de confianza de que un componente, dispositivo, persona u otra entidad es quien/lo que dice ser. El algunas situaciones, la autentificación puede considerarse algunas veces como sinónimo de identidad.

Autorización se refiere a la concesión de un nivel de control de acceso y responde a la pregunta de qué acciones puede estar autorizada a realizar una entidad. Por ejemplo, la autorización puede indicar si la entidad tiene permiso para acceder a datos seleccionados, cuándo y durante cuánto tiempo.

CAS (Sistema de Acceso Condicional). El CAS se refiere a tecnologías orientadas a controlar el acceso a servicios tales como los servicios de televisión digital y similares, encriptando la programación transmitida. No obstante, el CAS no está dirigido solamente a la televisión. Puede comprender emisiones de radio digitales, radiodifusión de datos digitales, información no radiodifundida, servicios interactivos y similares. Así, el CAS puede comprender acceso a datos de transmisión continua como los descritos en la presente memoria.

Renovación rápida se refiere a la provisión de generación de claves, nuevas claves y nuevos mecanismos de seguridad a un dispositivo o sistema cliente y similar. En una forma de realización, la renovación rápida dinámica proporciona el mecanismo de seguridad renovado de base aleatoria para crear un entorno impredecible previsto para terceros, por ejemplo piratas informáticos.

La DRM (Gestión digital de derechos) comprende un mecanismo alternativo basado en archivos para la protección de datos multimedia. La DRM comprende, por ejemplo, protección del propio contenido, por ejemplo datos de transmisión continua. En una forma de realización puede enviarse un archivo de licencia, o similar, para permitir a un usuario reproducir el contenido, ya sea de forma conjunta o cuando el usuario intenta reproducir el contenido. El contenido, por ejemplo datos de transmisión continua, puede encriptarse y las propiedades de encriptación pueden persistir mientras el contenido viaja entre redes, servidores, y hasta un cliente. La DMR, tal como se describe en la presente memoria, puede utilizar una tarjeta inteligente virtual para permitir la gestión y la protección del contenido.

Los ECM (Mensajes de Control de Titularidad) comprenden datos encriptados asociados con habilitaciones, por ejemplo testigos, restricciones de acceso, claves deencriptación/contenido, etc.

Los EMM (Mensajes de Gestión de Titularidad) comprenden datos encriptados tales como testigos, restricciones de acceso, claves de encriptación/contenido, etc.

La Detección de intrusión comprende los mecanismos para detectar situaciones que pueden violar la política de seguridad y otras protecciones.

No rechazo comprende unos mecanismos dirigidos a garantizar que el usuario, el consumidor, el cliente y similares no pueden negar la validez de su firma digital. Una forma de realización utiliza dos claves diferentes. Una puede estar bajo custodia de un tercero y utilizarse para acciones sin firma. La segunda puede carecer de mecanismos de recuperación y utilizarse para acciones con firma. En esta forma de realización, en la cual el usuario puede controlar en solitario la clave de firma, puede obtenerse el no rechazo utilizando una clave secreta de firma que sólo tenga el usuario pero que pueda ser verificada. Cuando la validez de la firma pueda ser decisiva, puede utilizarse una clave separada que sólo conocerá el usuario pero que podrá ser verificada por el soportador de la clave. En otra forma de realización, el soportador de la clave puede rechazar la validez de la firma basándose en la aptitud de una entidad con privilegios suficientes para duplicar la clave secreta.

En una forma de realización del procedimiento según la invención y el servidor de transmisión continua, el vídeo puede almacenarse sin encriptar en los servidores; los archivos sólo podrán recuperarse a través del software del servidor. El servidor según la invención será el responsable de (1) negociar un conjunto de claves de encriptación y (2) de encriptar el flujo de datos "sobre la marcha", haciendo los paquetes de datos que recorren realmente la red inútiles para cualquier ordenador que no sea el dispositivo previsto. Un encriptación estándar es la TRIPLE DES con una clave de 168 bits. El servidor utilizará recursos de red muy inferiores a los de otros protocolos TCP (por ejemplo http).

El software de cliente será el responsable de desencriptar el flujo de datos y reproducirlo. Las claves de encriptación utilizadas pueden ser diferentes cada vez que se accede al flujo de datos. Cada vez que se ejecuta el cliente se crea una clave de encriptación diferente para que el cliente no pueda reproducir flujos de datos anteriores si se han guardado de algún modo en el disco.

Entorno ilustrativo

Con respecto a la figura 1, muestra un esquema de una forma de realización del componente del cliente del procedimiento según la invención y del servidor de transmisión continua autorizado para recibir y ver y/o acceder de otro modo a un flujo de datos encriptado. El cliente guarda una lista de todos los flujos de datos y testigos actuales. Esta información se almacena en el módulo de almacenamiento de testigos 100. Esta lista comprenderá los tres artículos siguientes: (1) el URI, (2) el testigo para este URI y (3) la fecha de vencimiento dada por el servidor. En una forma de realización, podría no ser deseable que el cliente pudiera determinar de algún modo si el testigo es válido o no. Por esta razón y por la necesidad de eliminar todos los testigos vencidos, el servidor indica la fecha de vencimiento. Esta información es utilizada por el cliente para visualizar información. La fecha de vencimiento en si misma podría no ser devuelta nunca al servidor y el propio servidor verifica que el testigo pasado es válido. Los ejemplos de dispositivos de módulo que pueden utilizarse como módulos de almacenamiento de testigos comprenden, por ejemplo, memoria RAM, almacenamiento secundario (disco duro) e integrado con software que proporciona un inventario del almacenamiento de testigos y efectúa un seguimiento de las fechas de vencimiento.

El cliente se comunica con una interfaz de usuario (110). El cliente puede disponer de una interfaz de usuario que proporcionará la experiencia de usuario adecuada. La interfaz tendrá capacidad para revisar los flujos válidos actuales o para conectar con el servidor para buscar otros flujos que podrían ser vistos. La interfaz de usuario del cliente 110 se comunica con un módulo de control de pantalla local 130 y un módulo de protocolo de control de flujo 120. El cliente debe poder establecer una sesión de comunicación con el servidor, así como controlar el flujo de datos procedente del servidor cuando el flujo esta siendo visualizado. El módulo de protocolo de control 120 crea la conexión inicial conectando con el servidor y pasando el URI, el testigo y la información de usuario solicitados. A continuación, el módulo de protocolo de control 120 negocia un conjunto de claves de encriptación y controla el flujo de datos procedente del servidor. Los ejemplos de dispositivos de módulo de protocolo de control de flujo 120 dentro de un componente del cliente que puede ser utilizado para negociar un conjunto de claves de encriptación y control del flujo de datos procedente de un servidor comprenden, por ejemplo, la memoria RAM y la tarjeta de interfaz de red o módem. El software puede monitorizar la velocidad de los datos que se están recibiendo enviando al servidor de transmisión continua estadísticas de red, información asociada con la memoria intermedia, incluyendo el porcentaje completado, el porcentaje restante y similares, así como otras características del cliente. El módulo de control de visualización 130 controla la visualización de los datos, y puede pausar, detener o reiniciar el flujo de datos. Los ejemplos de módulos de control de visualización adecuados para su utilización dentro del componente del cliente comprenden memoria RAM, y la tarjeta de vídeo. El software que se ejecuta en este módulo convertirá los datos que se están enviando desde el servidor a un formato que puede ser visualizado para el usuario.

El módulo de visualización 140 visualiza datos de vídeo y de audio. El módulo de memoria intermedia de entrada 150 es un módulo que comprende la memoria intermedia de flujo. La memoria intermedia de flujo puede comprender una memoria intermedia circular de datos desencriptados desde la que el módulo de control de visualización lee y en la que el módulo de desencriptación escribe. Los ejemplos de dispositivos de módulo que pueden utilizarse para incluir una memoria intermedia circular o datos desencriptados comprenden, por ejemplo, la memoria RAM. Cuando se reciben los paquetes del servidor, antes de que los datos se coloquen en la memoria intermedia de entrada, los datos del interior del paquete son desencriptados por el módulo de desencriptación 160, utilizando las claves negociadas por el módulo de protocolo de control de flujo 120.

El módulo de desencriptación 160 puede implementarse utilizando virtualmente cualesquiera mecanismos de desencriptación, incluyendo los que se encuentran disponibles comercialmente. Por ejemplo, los módulos SSL, DES y RSA se encuentran disponibles comercialmente y son adecuados para su utilización como módulo de desencriptación.

Finalmente, por la parte del componente del cliente existe un módulo de recepción de flujos de datos 170. Este módulo procesa la recepción de los paquetes de datos enviados por el servidor.

Los ejemplos de dispositivos de módulo adecuados que pueden utilizarse como módulo de recepción de flujos de datos dentro del componente del cliente comprenden, por ejemplo, la memoria RAM. El software incluido en este módulo puede guardar los datos recibidos por el cliente en un formato que puede ser utilizado por los módulos posteriores.

Haciendo referencia a la figura 2, el módulo de conexión de control del cliente 200 procesará las comunicaciones de control entre el cliente y el servidor. El cliente y el servidor negociarán un conjunto de claves de encriptación. El cliente enviará información de usuario, el URI y el testigo al servidor de transmisión continua, a través del módulo de conexión de control del cliente 200. Desde este módulo 200 pueden controlarse los datos enviados al cliente (es decir, el flujo de datos puede pausarse, detenerse o reiniciarse). Los dispositivos de hardware adecuados para utilización como módulo de conexión de control de cliente dentro del servidor de transmisión continua comprenden memoria RAM. Tales componentes de hardware permiten la ejecución de operaciones no específicas del hardware. El software se encuentra integrado en el módulo de conexión de control de cliente o cargado en él. El software funciona creando un proceso en el que el cliente y el servidor se comunican las condiciones de red actuales y modifican el flujo de datos correspondientemente.

El módulo de conexión de datos de cliente 210 funciona enviando paquetes de datos al cliente utilizando un protocolo sin conexión para reducir el recalentamiento del servidor. Los dispositivos de hardware adecuados para utilización como módulo de conexión de datos de cliente dentro del servidor de transmisión continua comprenden memoria RAM y las tarjetas de interfaz de red. Dicho hardware se encuentra integrado en el módulo de conexión de datos de cliente o se carga en el mismo. El software funciona creando un proceso en el que los datos encriptados se envían al dispositivo del cliente a través de paquetes de red.

El módulo de encriptación 220 utiliza las claves negociadas por el cliente/servidor para encriptar el flujo de datos cuando está siendo enviado al cliente. Esto permite la encriptación “sobre la marcha” y las claves de encriptación serán únicas para todas las conexiones cliente/servidor. Esto permite que el flujo fuente se almacene sin encriptar en el servidor, en el lugar adecuado. Los dispositivos de hardware adecuados para su utilización como módulo de encriptación dentro del servidor de transmisión continua comprenden memoria RAM y dispositivos de hardware de encriptación patentados. Tales componentes de hardware incluyen software que funciona efectuando la encriptación de datos real. El software puede encontrarse tanto integrado en el módulo de encriptación como cargado en el mismo. El software funciona creando un proceso en el que los datos que están siendo enviados al dispositivo se encriptan con las claves originalmente negociadas con el cliente y los datos de salida presentan un formato que no puede ser leído hasta ser desencriptado por el cliente.

El módulo de control de flujo 230 garantiza que el flujo de datos está siendo enviado por el servidor a la velocidad a la que el cliente está utilizando los datos. La memoria intermedia del cliente necesita estar llena siempre pero tampoco deben sobrescribirse los datos de transmisión continua. Por lo tanto, el módulo de control de flujo comunica con el módulo de encriptación 220 y utiliza la retroalimentación obtenida del módulo de conexión de control del cliente 200. Los dispositivos de hardware adecuados para su utilización como módulo de control de flujo dentro del servidor de transmisión continua comprenden memoria RAM. El software puede estar integrado en el módulo de control e flujo o cargado en el mismo. El software funciona creando un proceso en el cual se regula el flujo de datos del servidor al cliente.

La memoria intermedia de lectura del sistema de archivos 240 es para el rendimiento del servidor. En la memoria pueden almacenarse pequeñas cantidades de datos leídos del archivo en lugar de tener que abrir constantemente archivo por archivo del sistema. El módulo de sistema de archivos 250 es el responsable de la lectura de los datos procedentes del flujo fuente en el medio de almacenamiento o en otro lugar. El módulo del sistema de archivos comunica con el módulo de conexión de control de cliente 200 para abrir los URI y con el módulo de interfaz de usuario 260 para configuraciones de rutas de archivo. Los dispositivos de hardware adecuados para su utilización como módulo del sistema de archivos dentro del servidor de transmisión continua comprenden memoria RAM. Tales componentes de software comprenden software que funciona para permitir el acceso a los flujos de datos. Dicho software puede estar integrado en el módulo de sistema de archivos o cargado en el mismo. El software funciona creando un proceso en el que los datos guardados en el dispositivo de almacenamiento secundario pueden cargarse en la memoria RAM para ser enviados al módulo de encriptación.

El servidor de transmisión continua además dispone un módulo 260 de interfaz de usuario para establecer opciones de servidor tales como el puerto al cual conectarse y la ubicación del flujo fuente. Los dispositivos de hardware adecuados para su utilización como módulo de sistema de archivos comprenden memoria RAM. El software se encuentra integrado en el dispositivo modular o se carga en el mismo. El software funciona para crear un proceso en el cual el usuario del software del servidor puede puede indicar al módulo de sistema de archivos dónde debe ir para encontrar los flujos de datos.

Haciendo referencia a la figura 3, el servidor de transacciones comprenden cuatro componentes de módulo. Para acceder a un flujo de vídeo, el cliente debe obtener primero un testigo de transacción. El testigo de transacción puede basarse en un esquema de pay-per-view en el cual el testigo será válido para un período de tiempo determinado. El

tiempo durante el cual es válido un testigo depende de la selección del usuario y de las opciones disponibles para el flujo de datos seleccionado. El usuario se pone en contacto con el servidor de transacciones mediante el módulo de interacción de cliente 300, con la información de usuario y el URI. El servidor de transacciones determinará las opciones de tiempo disponibles para testigo y las presentará al usuario. Una vez que el usuario ha seleccionado el límite de tiempo requerido, la solicitud se transmite al módulo de verificación de usuario 310. Los dispositivos de hardware adecuados para su utilización como módulo de interacción de cliente dentro del servidor de transacciones comprenden memoria RAM. El software puede estar integrado en el módulo de interacción de cliente o cargado en el mismo. El software funciona creando un proceso en el cual la información del usuario se verifica comparándola con la base de datos y se crea un testigo válido basándose, en parte, en las opciones solicitadas por el usuario.

El módulo de verificación de usuario 310 examina la información de usuario transmitida comparándola con la base de datos de usuarios para comprobar si el usuario es válido o no. La base de datos de usuarios reside en la memoria del módulo de verificación de usuario. Los dispositivos de hardware adecuados para su utilización como módulo de verificación de usuario dentro del servidor de transacciones comprenden memoria RAM. El software se encuentra integrado en el módulo de verificación de usuario o cargado en el mismo. El software funciona creando un proceso en el cual se verifica el testigo transmitido. El módulo de creación de URI 320 y el módulo de creación de testigos 330 están vinculados y el testigo se basa, en parte, en el URI solicitado. Esto significa que el testigo es único para el URI solicitado y no puede ser utilizado para ningún otro flujo. A continuación, esta información se transmite de vuelta al cliente a través del módulo 300. Los dispositivos de hardware adecuados para su utilización como módulo de creación de URI y módulo de creación de testigos se encuentran ambos ubicados dentro del servidor de transacciones y comprenden memoria RAM. Tales componentes de hardware pueden comprender software que funciona dentro de la memoria RAM. Esoftware puede estar integrado en el módulo de creación de URI o módulo de creación de testigos, o cargado en el mismo. El software funciona creando un proceso en el cual se crea un URI válido para el flujo multimedia que el usuario ha seleccionado.

Operaciones ilustrativas

Haciendo referencia a la figura 4, se ejecuta el cliente 400 y se carga con un URI y un testigo 410. El cliente clica dos veces sobre la icona de cliente (no) o lanza mediante un servidor multimedia (sí). Si el servidor multimedia lanza el cliente, los parámetros de la línea de comandos del cliente presentarán el URI y el testigo solicitados. Una presentación de ventana (420) lista todos los flujos de datos adquiridos (y actuales) disponibles para visualización, o interactúa de otro modo. El usuario podrá seleccionar el acceso a un flujo de datos clicando sobre el título del flujo. La pantalla espera la entrada del usuario (430) y el usuario selecciona un flujo de datos u otra opción de verificación (440). Si se selecciona otra opción de verificación. Se ejecuta la solicitud del usuario (450) y vuelven a visualizarse los flujos de datos de vídeo con el módulo 420.

Si el usuario lanza un flujo de datos (selecciona "sí" en 410) se guardan un URI y un testigo en la lista de flujos adquiridos para que puedan ser vistos en un momento posterior 460. Se abre una conexión con el servidor de transmisión continua y el URI, el testigo y la información de usuario se envían al servidor de transmisión continua 470. El servidor de transmisión continua reconoce la combinación de URI y testigo válida (o inválida) 480. Si el testigo no es válido o ha caducado, el servidor cerrará la conexión y el cliente volverá atrás y visualizará todos los flujos de datos disponibles para ser visualizados. Si el servidor reconoce una combinación de URI y testigo válida, el cliente empezará a recibir datos del servidor de transmisión continua y los visualizará 490.

Si el flujo de datos termina o el usuario selecciona cualquiera de las opciones de flujo disponibles, como pausa, paro, reproducción o reinicio 500, el flujo se detendrá y esperará una nueva entrada del usuario. Si el flujo ha terminado la reproducción 510, el proceso vuelve atrás a la lista de flujos disponibles 420 o sigue visualizando el flujo de datos 490 procesando una solicitud del usuario 520 y seguidamente volviendo a reproducir el flujo 490.

Haciendo referencia a la figura 5 y al proceso que se ejecuta mediante el servidor de transmisión continua, se produce una primera conexión con el módulo de control de cliente 200, 600 para permitir al cliente establecer una conexión con el servidor de transmisión continua. El cliente proveerá el URI, el testigo y la información de usuario 610 del usuario 470. El servidor de transmisión continua determina si el testigo y el URI son válidos 620. Si el testigo no es válido o ha caducado, la conexión con el cliente se cerrará con un mensaje de error adecuado 630. Si el testigo es válido, se negociará con el cliente un conjunto de claves de encriptación únicas 640. Se abrirá un URI y se leerán los datos de transmisión continua en la memoria intermedia 650.

El módulo de control de flujo de cliente 230 se ocupa de que el cliente y el servidor de transmisión continua dispongan de una conexión de control de flujo establecida para garantizar que el flujo de datos sale del servidor de transmisión continua a una velocidad sustancialmente igual a la velocidad con la que se utiliza el flujo de datos en el extremo cliente 660. De este modo se direccionan las salidas de ancho de banda y se garantiza que la memoria intermedia de reproducción del cliente no se sobrescriba. Por lo tanto, el mecanismo de control de flujo de cliente 660 utiliza el módulo de control de flujo de cliente 230 para obtener la retroalimentación desde la memoria intermedia de datos del cliente 710 y controlar que la velocidad del flujo de datos mantenga la memoria intermedia del cliente tan llena como sea posible. Si en este momento el cliente no puede aceptar más datos, vuelve al módulo de control de flujo para indicar 670 que debe disminuir la velocidad de transferencia de datos o debe efectuarse una pausa. Si el cliente puede aceptar más datos 680, el flujo de control de datos de cliente determinará primero si hay más datos para transferir 680. Si no hay más datos para transferir, la transferencia de datos puede haberse completado y la conexión

con el cliente se cerrará 690. Si todavía quedan datos para enviar, se encriptarán los datos que se encuentran esperando en la memoria intermedia de transmisión 700 y los datos encriptados se enviarán al cliente 710.

Con respecto a la figura 6, en el servidor de transacciones, el cliente se conecta primero con el servidor de transacciones, por ejemplo a través de una página web 800. En una forma de realización, el servidor de transacciones se implementará con scripts ASP. No obstante, la invención no se limita a los mismos y puede utilizarse virtualmente cualquier mecanismo. El cliente envía el URI de solicitud y la información de usuario a través argumentos de la línea de comandos ASP 810 y el módulo de verificación de usuarios del servidor de transacciones 310 determinará los límites de tiempo de los testigos disponibles y los visualizará para el usuario con fines de selección. El servidor de transacciones buscará la información de usuario 820 en una base de datos del módulo de verificación de usuarios 310. Los ejemplos de búsqueda de información de usuario son válidos tanto si existe una cuenta del usuario como si no (por ejemplo, según el servidor de transacciones existe una cuenta) 830. Si no existe una cuenta del usuario 840, se abrirá una transacción para crear una nueva página de cuenta y obtener información del usuario 840. Además, el módulo de verificación de usuarios del servidor de transacciones 310 determinará si el URI solicitado es gratuito 850. Si el URI debe pagarse 860, el módulo de verificación de usuarios del servidor de transacciones 310 cargará el importe en la tarjeta de crédito registrada en la base de datos. Este proceso creará un URI en el módulo de creación de URI 320 del servidor de transacciones.

Una vez proporcionado el URI y pagado u obtenido gratuitamente, se creará un testigo 870 en el módulo de creación de testigos 330. El testigo creado se enlazará con el URI y se seleccionará el límite temporal 880. Finalmente, se iniciará el visualizador en el dispositivo del cliente y se enviará al cliente junto con el URI y el testigo creado.

Componentes del cliente contenidos en una Tarjeta Virtual Ilustrativa

Los componentes del cliente descritos anteriormente mediante consideración conjunta de la figura 1 pueden utilizarse en una variedad de sistemas cliente. Tales sistemas cliente pueden comprender dispositivos que normalmente se conectan utilizando medios de comunicaciones alámbricos tales como ordenadores personales, sistemas multiprocesadores, electrónica de consumo programable o basada en microprocesadores, set top box, dispositivos de televisión interactiva, módulos e interfaces de punto de despliegue, PC de red y similares. Tales dispositivos también pueden comprender dispositivos que normalmente se conectan utilizando medios de comunicaciones inalámbricos, por ejemplo, teléfonos móviles, teléfonos inteligentes, radioavisadores, walky talky, dispositivos de radiofrecuencia (RF), dispositivos de infrarrojos (IR), CB, dispositivos integrados que combinan uno o más de los dispositivos anteriores, o virtualmente cualquier dispositivo móvil y similares. Similarmente, los sistemas cliente que pueden utilizar los componentes del cliente de la figura 1 pueden consistir en cualquier dispositivo capaz de conectarse utilizando un medio de comunicaciones alámbrico o inalámbrico, por ejemplo un PDA, un PC de bolsillo, un ordenador vestible y cualquier otro dispositivo equipado para comunicarse a través de un medio de comunicación alámbrico o inalámbrico.

Estos sistemas de cliente también pueden configurarse para utilizar datos transferidos por distintas razones, inclusive películas de entretenimiento, clips de audio y similares. En una forma de realización, los datos transferidos pueden comprender por lo menos una parte de los datos asociados con un servicio de televisión interactivo. Los datos transferidos pueden incluso estar asociados con actividades bancarias, actividades de comercio electrónico, y similares.

Además, los componentes del cliente de la figura 1 pueden disponerse en distintas configuraciones y pueden asociarse con diferentes arquitecturas. Por ejemplo, en una forma de realización, los componentes del cliente de la figura 1 pueden disponerse dentro de un sistema cliente que presenta una tarjeta inteligente virtual (VSC). Adicionalmente, los componentes del cliente pueden utilizarse junto con un entorno de televisión interactiva utilizando la VSC.

La figura 7 muestra una forma de realización de una disposición de esta clase para la VSC, incluida en un dispositivo cliente configurado para interactuar operativamente con un servidor de transacciones, de un modo sustancialmente similar al descrito anteriormente en relación con las figuras 2 a 6. El sistema cliente 7000 de la figura 7 puede comprender muchos más componentes de los que se representan. No obstante, los componentes representados son suficientes para dar a conocer una forma de realización ilustrativa de la puesta en práctica de la invención, pudiendo efectuarse variaciones en la disposición y el tipo de los componentes.

La utilización de la VSC descrita permite obtener privacidad (confidencialidad), integridad, oportunidad, control de acceso (autorización) y autentificación (identidad), así como renovación rápida, protección de copias por enlace cruzado y gestión digital de derechos, y mayor capacidad, flexibilidad y aptitud para conectar con un dispositivo para aumentar la seguridad.

Como muestra la figura, el sistema cliente 7000 comprende el dispositivo cliente 7002. El dispositivo cliente 7002 comprende VSC 7004, detección de falsificaciones 7006, módulo de recepción de flujos de datos 7170, módulo de visualización 7140, módulo de control de visualización local 7130 e interfaz de usuario 7110. La VSC 7004 comprende módulos de control de flujo y comunicación 7010, gestión de mensaje seguro 7012, protección contra falsificaciones 7014, memoria intermedia de entrada del cliente 7150, gestor de testigos 7016, módulos criptográficos 7060, módulo de almacenamiento de testigos 7100, generador de claves 7018 y módulo de enlace 7020.

La interfaz de usuario 7110 funciona de forma sustancialmente similar a la interfaz de usuario 110 de la figura 1. La interfaz de usuario 7110 puede comprender diversos dispositivos de entrada de cliente, incluyendo un ratón, teclado,

micrófono, pantalla táctil, dispositivo de control remoto y similares, configurado para proporcionar la capacidad de seleccionar un flujo de datos, así como obtener información.

El módulo de control de visualización local 7130 funciona de forma sustancialmente similar al módulo de control de visualización local 130 de la figura 1. Es decir, el módulo de control de visualización local 7130 puede ser virtualmente cualquier dispositivo, software, combinación de software y hardware y similar que permita el control de una visualización de datos y pueda efectuar pausas, parar, iniciar y reiniciar un flujo de datos.

El módulo de visualización 7140 funciona de forma sustancialmente similar al módulo de visualización 140 de la figura 1. Es decir, el módulo de visualización 7140 permite la presentación del flujo de datos, incluyendo datos de vídeo, datos de audio y similares, para un usuario. El módulo de visualización 7140 puede, por ejemplo, permitir la presentación de un flujo de datos de televisión interactiva.

El módulo de recepción de flujos de datos 7170 funciona de modo sustancialmente similar al módulo de recepción de flujos de datos 170 de la figura 1. Es decir, el módulo de recepción de flujos de datos 7170 está configurado para gestionar la recepción de paquetes de datos asociada con el flujo de datos enviado por el servidor. El módulo de recepción de flujos de datos 7170 puede estar configurado, además, para suministrar los paquetes de datos recibidos al módulo de control de flujo y comunicación 7010.

El módulo de almacenamiento de testigos 7100 está configurado para funcionar de forma sustancialmente similar al módulo de almacenamiento de testigos 100 de la figura 1. Es decir, el módulo de almacenamiento de testigos 7100 está configurado para proveer un almacenamiento seguro de URI, testigos asociados con un URI guardado, una fecha de vencimiento asociada con el testigo y similares. Además, el módulo de almacenamiento de testigos 7100 también está configurado para proveer un almacenamiento local seguro estrechamente vinculado con el dispositivo cliente 7002. El módulo de almacenamiento de testigos 7100 puede implementarse en forma de archivo, carpeta, base de datos o similar. El enlace con el sistema cliente se realiza mediante el módulo de enlace 7020. Puede obtenerse seguridad local utilizando uno de los diferentes sistemas de encriptación u ocultación y a través de la utilización de diversos recursos de red.

El módulo de enlace 7020 está configurado para identificar de forma única al dispositivo cliente 7002, el sistema servidor o similar. En una forma de realización, esto se consigue utilizando una huella digital. Una huella digital puede consistir en diversos elementos específicos de cada huella digital. Tales elementos se denominan “crestas” en el presente documento. Cada cresta comprende un elemento de una huella digital que provee información de la huella digital que la hace única entre otras huellas digitales. Algunos ejemplos de crestas comprenden un número de serie de hardware, número de versión del sistema operativo, dirección del protocolo de internet, tamaño físico de la memoria y similares. Cada cresta comprendida en la huella digital afina la identidad del sistema de modo que puede ser identificada de forma única dentro de un sistema. Las combinaciones de todas las huellas digitales pueden crear una huella manual o huella digital del sistema, que identifica de forma única un ordenador personal, un servidor, un dispositivo cliente, un set top box o un dispositivo similar dentro del sistema. El orden de cada uno de los grupos de huellas digitales y crestas individuales puede afectar a la huella digital del sistema o huella manual resultante. Es decir, cada usuario del módulo de enlace 7020 puede generar una huella digital única y la consiguiente huella manual aunque la información de crestas común utilizada sea la misma.

La utilización de la huella digital generada conecta la VSC 7004 con un dispositivo específico, por ejemplo el dispositivo cliente 7002, de modo que no funcionará adecuadamente si se clona y se intenta ejecutarla en otro dispositivo. Este procedimiento elimina virtualmente el método corriente de los piratas informáticos de piratear físicamente tarjetas inteligentes.

En una forma de realización, la VSC 7004 puede combinarse con otro dispositivo, por ejemplo una tarjeta inteligente física, para incrementar adicionalmente las características de identidad segura de la tarjeta física respecto a la huella digital, manteniendo la flexibilidad y los poderes de la VSC 7004. Esto puede hacerse, por ejemplo, en un sistema en el cual la identidad del dispositivo es inherentemente débil, donde el coste y/o la conveniencia de la tarjeta física, o de otro dispositivo, no sean importantes.

El módulo de control de flujo y comunicación 7010 está configurado para permitir el control de flujo y comunicaciones de datos entre la VSC 7004 y los servidores de transacciones y transmisión continua. Como tal, el módulo de control de flujo y comunicación 7010 puede efectuar acciones sustancialmente similares a algunas acciones realizadas por el módulo de protocolo de control de flujo 120 de la figura 1. Es decir, el módulo de control de flujo y comunicación 7010 puede permitir una conexión inicial con un servidor y el paso de un URI, un testigo y una información de usuario solicitados.

El módulo de control de flujo y comunicación 7010 también puede permitir el control de flujo de los datos procedentes del servidor para garantizar que la velocidad de flujo mantiene la memoria intermedia del cliente (es decir, la memoria intermedia de entrada del cliente 7150) sustancialmente llena, de forma sustancialmente similar al módulo de protocolo de control de flujo 120 de la figura 1. El módulo de control de flujo y comunicación 7010 puede hacerlo, por ejemplo, monitorizando diversas características, tales como la velocidad a la que se reciben los datos, estadísticas de red, estadísticas de memoria intermedia de entrada, etc. Como tal, el módulo de control de flujo y comunicación 7010 puede permitir una pregunta de la memoria intermedia de entrada 7150 para determinar el porcentaje lleno, la

velocidad de llenado, el porcentaje de espacio restante en la memoria intermedia y, entonces, el módulo de control de flujo y comunicación 7010 puede disponer para el servidor una métrica de control de flujo basada en las características monitorizadas, encriptada o sin encriptar. Si la información se proporciona encriptada, el módulo de control de flujo y comunicación 7010 puede utilizar un gestor de mensaje seguro 7012 para garantizar que la información es segura.

El gestor de mensaje seguro 7012 está configurado para proporcionar un medio seguro para el intercambio de mensajes. Aunque no se representa, el gestor de mensaje seguro 7012 interactúa con otros componentes diversos de la VSC 7004 cuando se requiere para garantizar que se realiza la autentificación mutua de las partes finales y que se mantiene la privacidad de los mensajes.

El gestor de testigos 7016 está configurado para gestionar la recepción, almacenamiento, envío e interpretación de testigos y habilitaciones similares. Como tal, el gestor de testigos 7016 puede realizar diversas acciones relacionadas con el módulo de protocolo de control de flujos 120 de la figura 1. Por ejemplo, el gestor de testigos 7016 puede pasar al servidor el URI, el testigo y la información de usuario solicitados. El gestor de testigos 7016 también puede negociar un conjunto de claves de encriptación con el servidor, utilizando módulos criptográficos 7060 y/o el generador de claves 7018. Además, el gestor de testigos 7016 puede utilizar el gestor de mensaje seguro 7012 para facilitar comunicaciones seguras entre un servidor y un dispositivo cliente 7002.

Los Testigos ya se han descrito de manera breve anteriormente. No obstante, en una forma de realización, los testigos también pueden comprender un certificado digital que puede incluir información identificativa, claves de encriptación y similares, asociados con una autoridad de certificación pertinente. Una estructura de testigos de esta clase utilizada por la VSC 7004 proporciona un concepto único de cadenas de habilitación, que puede extenderse a un modelo comercial que supere al normalmente soportado por el modelo de autoridad de certificación tradicional. No obstante, la invención no está limitada por ello y la estructura de testigos puede utilizar virtualmente cualquier estructura configurada para asociar permisos de usuario a un flujo de datos específico.

El módulo criptográfico 7060 está orientado a proporcionar mecanismos criptográficos para efectuar tareas tales como encriptación, desencriptación, firmas digitales, generación de claves, etc. Por ejemplo, el módulo criptográfico 7060 puede comprender mecanismos criptográficos asimétricos configurados para proporcionar acciones criptográficas públicas/privadas basadas en claves. Las acciones criptográficas públicas/privadas comprenden generación de claves, firmas digitales, encriptación, desencriptación y comprobación de integridad. El módulo criptográfico 7060 también permite un intercambio seguro de claves de encriptación a través del gestor de testigos 7016 y del gestor de mensaje seguro 7012.

El módulo criptográfico 7060 puede además recibir contenido seguro del módulo de control de flujo y comunicación 7010, desencriptar el contenido seguro y enviar el contenido desencriptado a la memoria intermedia de entrada del cliente 7150.

La memoria intermedia de entrada del cliente 7150 funciona sustancialmente de modo similar a la memoria intermedia de cliente 150 de la figura 1. Es decir, la memoria intermedia del cliente 7150 está configurada para comprender la memoria intermedia de transferencia. Es importante tener en cuenta que, aunque la memoria intermedia de entrada del cliente 7150 se representa dentro de la VSC 7004, la invención no se limita a esta ubicación. Por ejemplo, la memoria intermedia de entrada del cliente 7150 puede residir dentro del dispositivo del cliente 7002 y fuera de la VSC 7004.

El módulo criptográfico 7060 está configurado para proveer diversas claves criptográficas, inclusive claves simétricas o privadas, claves asimétricas o públicas y similares. Aunque el módulo criptográfico 7060 puede utilizar virtualmente cualesquiera mecanismos criptográficos, en una forma de realización el módulo criptográfico 7060 utiliza AES para criptografía simétrica. En otra forma de realización, el módulo criptográfico 7060 utiliza RSA para acciones criptográficas asimétricas.

El generador de claves 7018 está configurado para utilizar el módulo criptográfico 7060 para facilitar la generación de claves criptográficas. Esta generación puede utilizar, por ejemplo, un mecanismo de renovación rápida con el cual puede realizarse una nueva generación de claves en un corto período de tiempo, en comparación con los mecanismos de sustitución de claves de tarjeta inteligente física. En una forma de realización, la generación de claves 7018 puede permitir la generación de claves nuevas en horas más que en días, semanas o incluso meses. En una forma de realización, para ocultar adicionalmente un punto de ataque potencial, se utiliza una renovación rápida dinámica, en la cual la regeneración de claves y similares se realiza con una base aleatoria para crear un entorno impredecible. En otra forma de realización, la renovación rápida dinámica también puede utilizarse para sustituir diversos componentes de software que además pueden minimizar un ataque. El uso de esta renovación rápida facilita la utilización de la VSC 7004 en otras situaciones diversas, inclusive transacciones bancarias, seguridad de empresas y comercio electrónico, y para la distribución de contenidos por los estudios.

La detección de falsificaciones 7006 y la protección contra falsificaciones 7014 pueden aplicarse a muchos puntos del sistema cliente 7000 para garantizar un infraestructura altamente segura. Normalmente, puede proveerse cierto nivel de protección o resistencia contra las falsificaciones como parte del software y/o del hardware de la VSC 7004. Como se representa. la VSC 7004 comprende protección contra falsificaciones 7014 para dotar de protección o resistencia contra falsificación y procedimientos de piratería informática. Esta protección puede comprender, además,

agentes configurados para realizar diversas acciones, inclusive detección de emuladores en circuito, detección de depuradores, resistencia contra depuradores, detección de la violación de espacio de memoria y protección contra la misma, así como detección de comportamientos de piratería a nivel de aplicación similares y protección contra los mismos.

La detección de falsificaciones 7006 está configurada para identificar falsificaciones de otros sistemas, por ejemplo en el dispositivo cliente 7002 y similares. Por ejemplo, en un entorno de televisión interactiva puede ser posible desplegar la detección de falsificaciones dentro de una red para monitorizar los intentos de clonación de tarjetas virtuales inteligentes y/o sus diversos componentes. La detección de falsificaciones 7006 puede proveer, además, una fuente temporal fiable, evitando ataques repetidos.

Funcionalmente, la VSC 7004 puede funcionar de forma sustancialmente similar a la descrita en la figura 4. Por ejemplo, como se describe en la figura 4, el cliente se carga con un URI y un testigo (ver bloque 400 de la figura 4). Esta acción puede surgir en la figura 7 a través de una interacción con el módulo de control de flujo y comunicación 7010, y también como interfaz de usuario 7110, módulo de visualización 7140 y similares.

Si el usuario lanza un flujo de datos en el bloque de decisión 410 de la figura 4, el proceso se desplaza al bloque 460, donde se guardan un URI y un testigo utilizando el gestor de testigos 7016 y el módulo de almacenamiento de testigos 7100. Pasando al bloque siguiente 470, el módulo de control de flujo y comunicación 7010, junto con el gestor de testigos 7016, envía el URI, el testigo y la información de usuario al servidor de straming.

Si, en el bloque de decisión 480, el servidor reconoce una combinación de URI y testigo válida, el procesamiento pasa al bloque 490 de la figura 4, donde los datos se transfieren desde el servidor de transmisión continua. Esta transferencia de datos puede ser recibida por el módulo de recepción de flujos de datos 7170 y enviada al módulo de control de flujo y comunicación 7010, donde puede producirse la desencriptación del flujo recibido utilizando los módulos criptográficos 7060. A continuación, el flujo de datos desencriptado puede colocarse en la memoria intermedia de entrada del cliente 7150. El módulo de control de flujo y comunicación 7010 provee información del flujo durante la transferencia de los datos para garantizar que la memoria intermedia del cliente se encuentra sustancialmente llena.

La memoria anterior, los ejemplos y los datos proporcionan una descripción completa de la producción y la utilización de la composición de la invención.

REIVINDICACIONES

1. Sistema para la comunicación de un flujo de datos a través de una red que comprende:

un dispositivo cliente (7002) configurado para efectuar acciones que incluyen:

permitir una solicitud de flujo de datos; y

un servidor de transmisión continua configurado para ejecutar acciones que incluyen:

validar un testigo para un flujo de datos solicitado;

caracterizado porque el sistema comprende:

una tarjeta inteligente virtual (7004) acoplada al dispositivo cliente (7002), estando configurada la tarjeta inteligente virtual (7004) para llevar a cabo acciones que incluyen:

negociar el testigo con el servidor de transmisión continua;

almacenar el testigo obtenido como respuesta a la negociación en un módulo de almacenamiento de testigos (7100) situado en el interior de la tarjeta inteligente virtual (7004);

enviar el testigo asociado junto con el flujo de datos solicitado;

recibir el flujo de datos solicitado, estando encriptado el flujo solicitado; y

proporcionar una métrica de control de flujo asociada con el flujo de datos; estando configurado el servidor de transmisión continua para efectuar acciones adicionales en el caso de que el testigo sea válido para el flujo de datos solicitado, comprendiendo dichas otras acciones:

transmitir el flujo de datos encriptado a la tarjeta inteligente virtual (7004) y

utilizar la métrica de control de flujo de la tarjeta inteligente virtual (7004), en parte para controlar el flujo de datos encriptados transferido a través de la red para mantener sustancialmente llena una memoria intermedia (7150) asociada con la tarjeta inteligente virtual (7004), para que el flujo de datos pueda recibirse a la velocidad a la cual el dispositivo cliente (7002) utiliza los datos.

2. Sistema según la reivindicación 1, en el que la tarjeta inteligente virtual (7004) comprende un gestor de testigos (7016) configurado para negociar el testigo con el servidor de transmisión continua.

3. Sistema según la reivindicación 1 ó 2, en el que la validación del testigo para el flujo de datos solicitado comprende asimismo la validación de un identificador asociado con una ubicación del flujo de datos con el testigo provisto.

4. Sistema según cualquiera de las reivindicaciones 1 a 3, en el que la tarjeta inteligente virtual (7004) comprende asimismo un módulo de control de flujo (7010) configurado para monitorizar por lo menos una estadística de red, y una característica de memoria intermedia para determinar la métrica de control de flujo.

5. Sistema según cualquiera de las reivindicaciones anteriores, en el que la tarjeta inteligente virtual (7004) comprende asimismo un módulo de enlace (7020) configurado para asociar de forma única la tarjeta inteligente virtual (7004) con el dispositivo cliente (7002).

6. Sistema según cualquiera de las reivindicaciones anteriores, en el que el servidor de transmisión continua está configurado para efectuar otras acciones, incluyendo la negociación de las claves de encriptación con la tarjeta inteligente virtual (7004) para su utilización en la encriptación del flujo de datos solicitado.

7. Sistema según la reivindicación 6, en el que la tarjeta inteligente virtual (7004) comprende asimismo un gestor de testigos (7016) configurado para interactuar con el servidor de transmisión continua para negociar las claves de encriptación.

8. Sistema según la reivindicación 6 ó 7, en el que el módulo de almacenamiento de testigos (7100) está configurado asimismo para almacenar por lo menos la información de usuario y/o un URI y/o las claves de encriptación.

9. Sistema según cualquiera de la reivindicaciones anteriores, en el que el testigo comprende asimismo un certificado digital.

10. Sistema según cualquiera de las reivindicaciones anteriores dispuesto para que el flujo de datos recibido por el dispositivo cliente (7002) pueda ser visto por un número predeterminado de visionados.

11. Señal de datos modulada para gestionar un flujo de datos a través de una red, comprendiendo la señal de datos modulada instrucciones dispuestas para efectuar unas acciones que incluyen:

solicitar el flujo de datos por un cliente (7000) que dispone de una tarjeta inteligente virtual (7004);

negociar entre la tarjeta inteligente virtual (7004) y un servidor un testigo asociado con el flujo de datos solicitado;

almacenar el testigo obtenido como respuesta a la negociación en el módulo de almacenamiento de testigos (7100) dentro de la tarjeta inteligente virtual (7004);

facilitar la determinación de la validez del testigo para el flujo de datos solicitado; y, si el testigo es válido para el flujo de datos solicitado,

facilitar la negociación de una clave de encriptación con la tarjeta inteligente virtual (7004);

facilitar la encriptación del flujo de datos cuando el flujo de datos se transfiere al dispositivo cliente (7000), efectuándose la encriptación del flujo de datos utilizando la clave de encriptación negociada;

proporcionar la tarjeta inteligente virtual (7004) una métrica de control de flujo asociada con el flujo de datos encriptado; y

controlar, mediante el servidor, una velocidad de flujo del flujo de datos encriptado, a través de la red hasta el cliente (7000), utilizando el servidor para ello la métrica de control de flujo, en parte para controlar la velocidad de flujo del flujo de datos encriptado de modo que la memoria intermedia del cliente se mantenga sustancialmente llena, con el fin de que el flujo de datos pueda ser recibido a la velocidad a la que el cliente (7000) utiliza los datos.

12. Señal de datos modulada según la reivindicación 11, configurada para permitir solamente un único visionado del flujo de datos del sistema.

13. Señal de datos modulada según la reivindicación 11 ó 12, en la que la acción de controlar la velocidad de flujo comprende asimismo la transmisión del flujo de datos encriptados al cliente (7000) a sustancialmente la misma velocidad a la que el flujo de datos encriptado es recibido por el cliente (7000).

14. Señal de datos modulada según cualquiera de las reivindicaciones 11 a 13, en la que la acción de proporcionar una métrica de control de flujo comprende asimismo la monitorización de por lo menos una estadística de red y/o una característica de memoria intermedia de cliente.

15. Dispositivo cliente (7002) para su utilización en la recepción de un flujo de datos a través de una red, que comprende:

una interfaz de usuario (7110) configurada para efectuar acciones que incluyen:

permitir una solicitud de flujo de datos;

caracterizado porque el dispositivo cliente (7002) comprende:

una tarjeta inteligente virtual (7004) acoplada a una interfaz de usuario (7110), configurada para efectuar acciones que incluyen:

negociar con un servidor un testigo asociado al flujo de datos solicitado;

almacenar el testigo obtenido como respuesta a la negociación en un módulo de almacenamiento de testigos (7100) situado en el interior de la tarjeta inteligente (7004);

utilizar el testigo para permitir la validación de la solicitud de flujo de datos;

si la solicitud es válida, recibir el flujo de datos del servidor; y

proporcionar al servidor una métrica que pueda ser empleada por el servidor para controlar la velocidad de flujo del flujo de datos, con el fin de mantener sustancialmente llena la memoria intermedia del cliente (7150) para que el flujo de datos pueda recibirse a la velocidad a la cual el dispositivo cliente (7002) utiliza los datos.

16. Dispositivo cliente según la reivindicación 15, en el que la interfaz de usuario (7110) está configurada para efectuar otras acciones que comprenden:

permitir un límite de tiempo seleccionado por el usuario para acceder al flujo de datos que debe ser suministrado al servidor, estando seleccionado el límite de tiempo por el usuario asociado con el testigo negociado, de modo que una vez expirado el límite de tiempo el acceso al flujo de datos es denegado.

17. Dispositivo cliente según la reivindicación 15 ó 16, en el que el testigo comprende unos permisos de usuario para el flujo de datos solicitado.

18. Dispositivo cliente según la reivindicación 17, en el que la información de usuario comprende información de la cuenta de usuario.

19. Dispositivo cliente según la reivindicación 15, en el que el testigo comprende un límite de tiempo seleccionado por el usuario para acceder al flujo de datos, siendo denegado el acceso al flujo de datos una vez expirado el límite de tiempo seleccionado por el usuario.

20. Dispositivo cliente según cualquiera de las reivindicaciones 15 a 19, en el que el flujo de datos recibido se encripta utilizando por lo menos uno de entre las encriptaciones siguientes: DES, Triple-DES y AES.

21. Dispositivo cliente según cualquiera de las reivindicaciones 15 a 20, en el que la tarjeta inteligente virtual (7004) se encuentra enlazada únicamente con el dispositivo cliente (7002).

22. Dispositivo cliente según cualquiera de las reivindicaciones 15 a 21, en el que la tarjeta inteligente virtual (7004) comprende asimismo un módulo de protección contra falsificación (7014) configurado para detectar falsificaciones y proteger contra ellas a la tarjeta inteligente virtual (7004).

23. Dispositivo cliente según cualquiera de las reivindicaciones 15 a 22, en el que la tarjeta inteligente virtual (7004) comprende la memoria intermedia de cliente (7150).

24. Procedimiento para comunicar un flujo de datos a través de una red que comprende las etapas siguientes:

solicitar el flujo de datos;

utilizar un testigo negociado asociado con el flujo de datos solicitado para permitir la validación de la solicitud del flujo de datos;

si la solicitud es válida, recibir el flujo de datos procedente de un servidor.

caracterizado porque presenta las etapas siguientes:

negociar con el servidor, mediante una tarjeta inteligente virtual (7004) acoplada al dispositivo cliente (7002), el testigo asociado con el flujo de datos solicitado;

almacenar en un módulo de almacenamiento de testigos (7100), situado en el interior de la tarjeta inteligente virtual (7004), el testigo obtenido como respuesta a la negociación; y

suministrar al servidor, por la tarjeta inteligente virtual (7004), una métrica que el servidor puede utilizar, en parte, para controlar la velocidad de flujo del flujo de datos, con el fin de mantener sustancialmente llena la memoria intermedia del cliente (7150) para que el flujo de datos pueda recibirse a la velocidad a la cual el dispositivo cliente (7002) utiliza los datos.

25. Procedimiento según la reivindicación 24, que comprende asimismo:

utilizar un gestor de testigos (7016) asociado con la tarjeta inteligente virtual (7004) para interactuar con el servidor para negociar las claves de encriptación que se pueden utilizar para encriptar el flujo de datos cuando se está transfiriendo el flujo de datos al dispositivo cliente (7002).

26. Procedimiento según la reivindicación 24 ó 25, en el que el módulo de almacenamiento de testigos (7100) está configurado, asimismo, para almacenar por lo menos información de usuario, y un URI y las claves de encriptación.

27. Procedimiento según cualquiera de las reivindicaciones 24 a 26, en el que la tarjeta inteligente virtual (7004) está enlazada con el dispositivo cliente (7002).

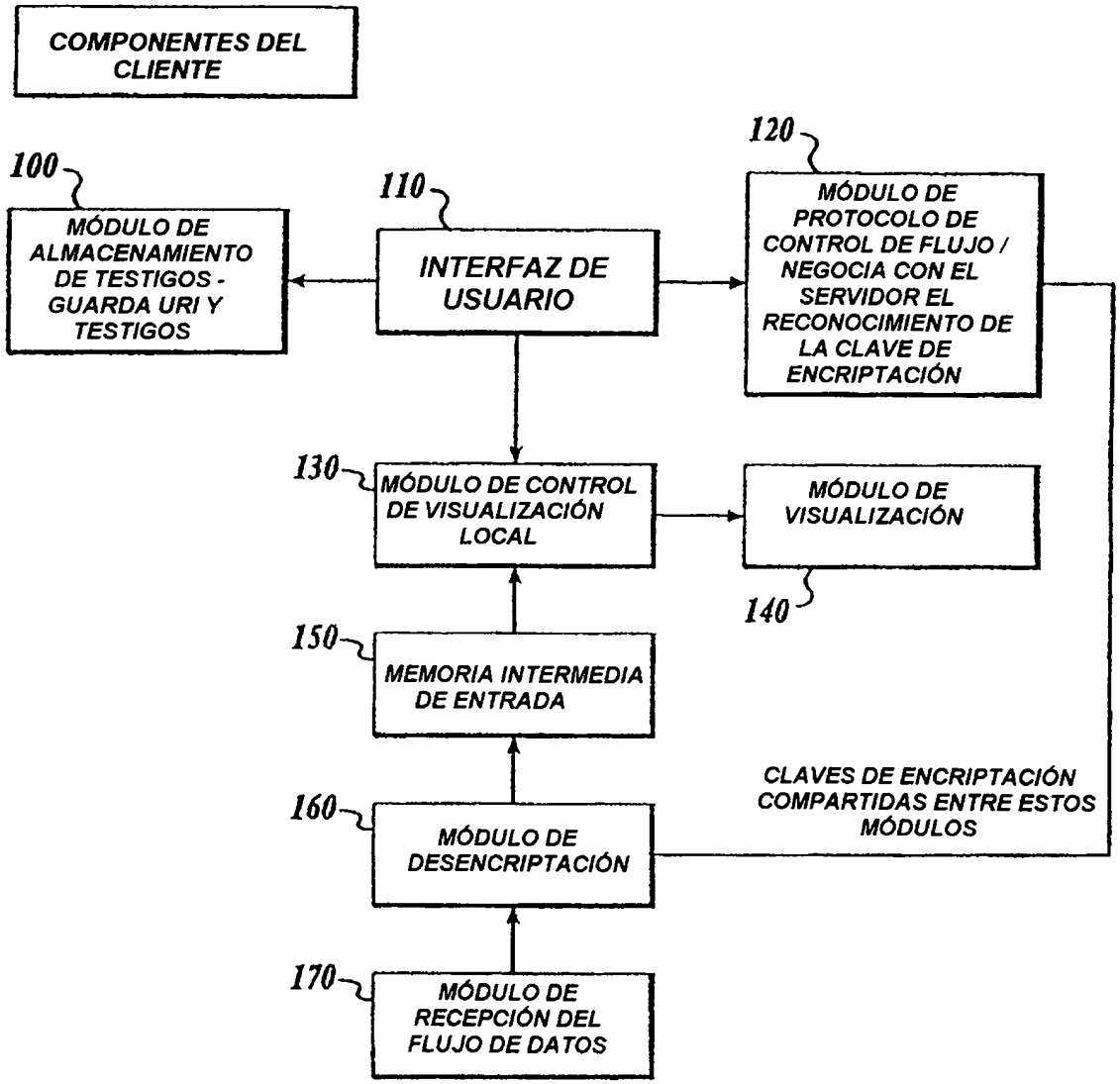
COMPONENTES DEL CLIENTE
100
MÓDULO DE ALMACENAMIENTO DE TESTIGOS - GUARDA URI Y TESTIGOS
110
INTERFAZ DE USUARIO
120
MÓDULO DE PROTOCOLO DE CONTROL DE FLUJO / NEGOCIA CON EL SERVIDOR EL RECONOCIMIENTO DE LA CLAVE DE ENCRIPTACIÓN
130
MÓDULO DE CONTROL DE VISUALIZACIÓN LOCAL
MÓDULO DE VISUALIZACIÓN
140
150
MEMORIA INTERMEDIA DE ENTRADA
160
MÓDULO DE DESENCRIPTACIÓN
CLAVES DE ENCRIPTACIÓN COMPARTIDAS ENTRE ESTOS MÓDULOS
170
MÓDULO DE RECEPCIÓN DEL FLUJO DE DATOS

Fig. 1.

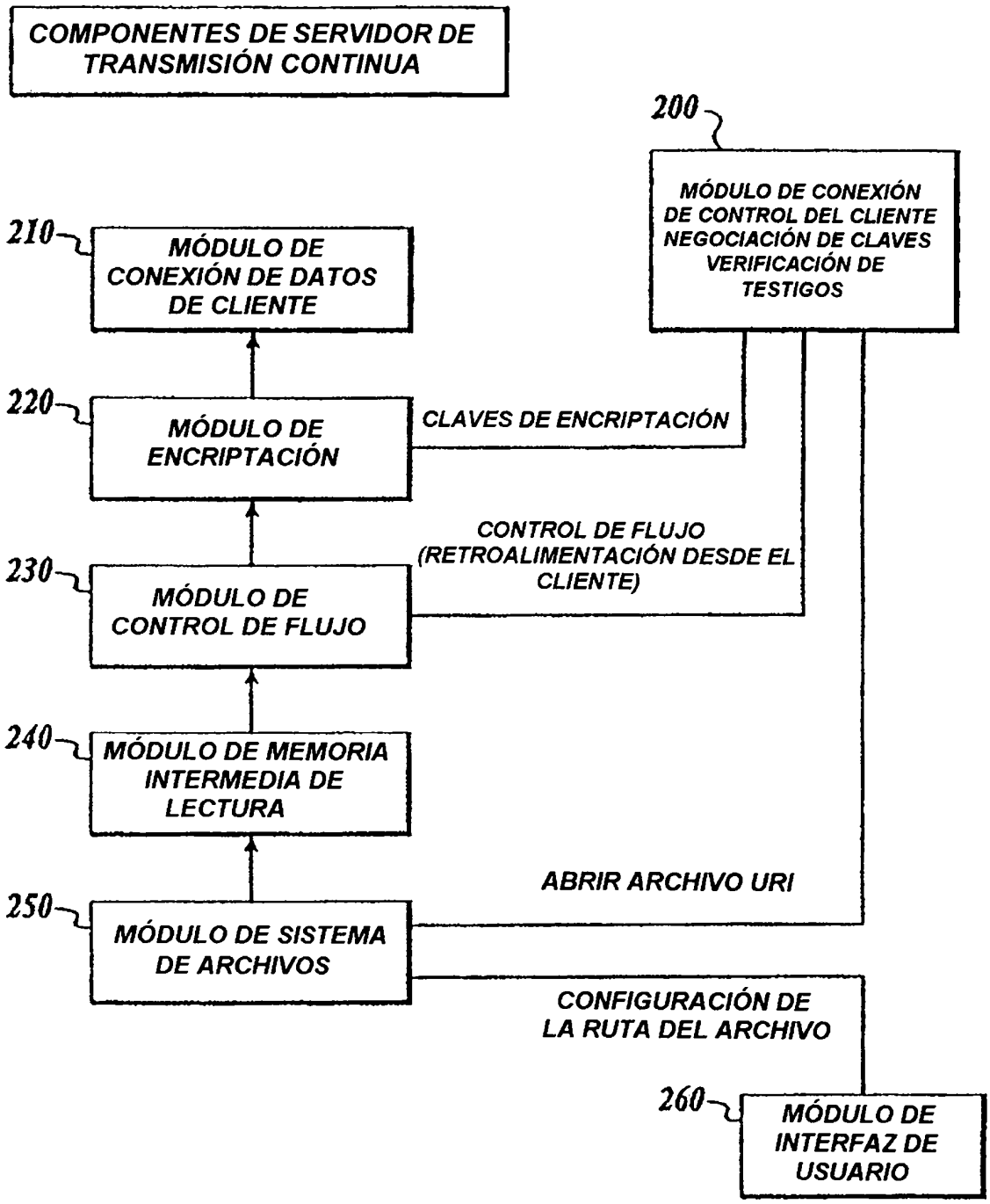
COMPONENTES DE SERVIDOR DE TRANSMISIÓN CONTINUA
200
MÓDULO DE CONEXIÓN DE CONTROL DEL CLIENTE NEGOCIACIÓN DE CLAVES VERIFICACIÓN DE TESTIGOS
210
MÓDULO DE CONEXIÓN DE DATOS DE CLIENTE
220
MÓDULO DE ENCRIPTACIÓN
CLAVES DE ENCRIPTACIÓN
CONTROL DE FLUJO (RETROALIMENTACIÓN DESDE EL CLIENTE)
230
MÓDULO DE CONTROL DE FLUJO
240
MÓDULO DE MEMORIA INTERMEDIA DE LECTURA
ABRIR ARCHIVO URI
250
MÓDULO DE SISTEMA DE ARCHIVOS
CONFIGURACIÓN DE LA RUTA DEL ARCHIVO
260
MÓDULO DE INTERFAZ DE USUARIO

Fig. 2.

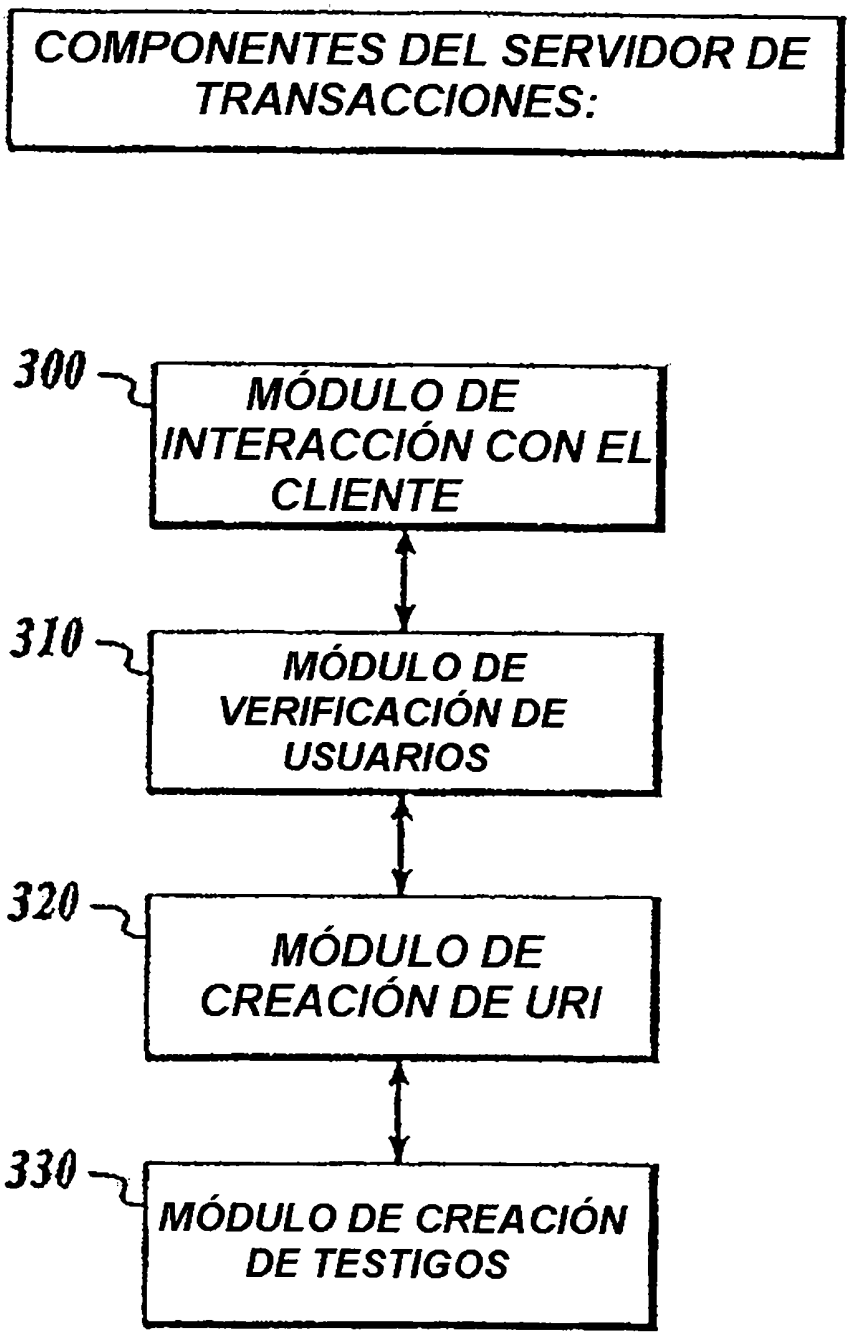
COMPONENTES DEL SERVIDOR DE TRANSACCIONES:
300
MÓDULO DE INTERACCIÓN CON EL CLIENTE
310
MÓDULO DE VERIFICACIÓN DE USUARIOS
320
MÓDULO DE CREACIÓN DE URI
330
MÓDULO DE CREACIÓN DE TESTIGOS

Fig. 3.

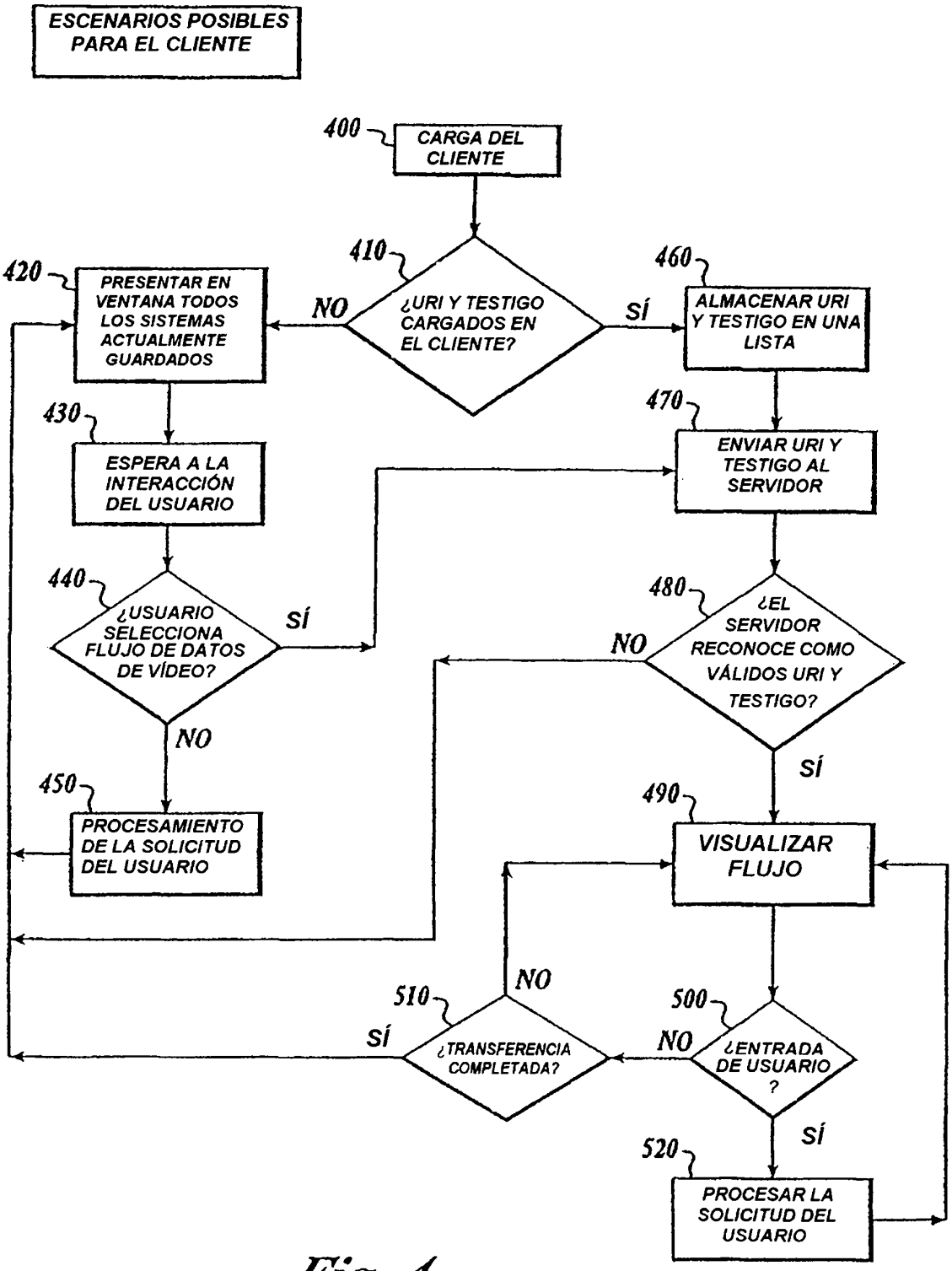
ESCENARIOS POSIBLES PARA EL CLIENTE
400
CARGA DEL CLIENTE
410
¿URI Y TESTIGO CARGADOS EN EL CLIENTE?
NO
SÍ
420
PRESENTAR EN VENTANA TODOS LOS SISTEMAS ACTUALMENTE GUARDADOS
460
ALMACENAR URI Y TESTIGO EN UNA LISTA
430
ESPERA A LA INTERACCIÓN DEL USUARIO
470
ENVIAR URI Y TESTIGO AL SERVIDOR
440
¿USUARIO SELECCIONA FLUJO DE DATOS DE VÍDEO?
SÍ
NO
480
¿EL SERVIDOR RECONOCE COMO VÁLIDOS URI Y TESTIGO?
NO
SÍ
450
PROCESAMIENTO DE LA SOLICITUD DEL USUARIO
490
VISUALIZAR FLUJO
510
¿TRANSFERENCIA COMPLETADA?
NO
SÍ
500
¿ENTRADA DE USUARIO ?
NO
SÍ
520
PROCESAR LA SOLICITUD DEL USUARIO

Fig. 4.

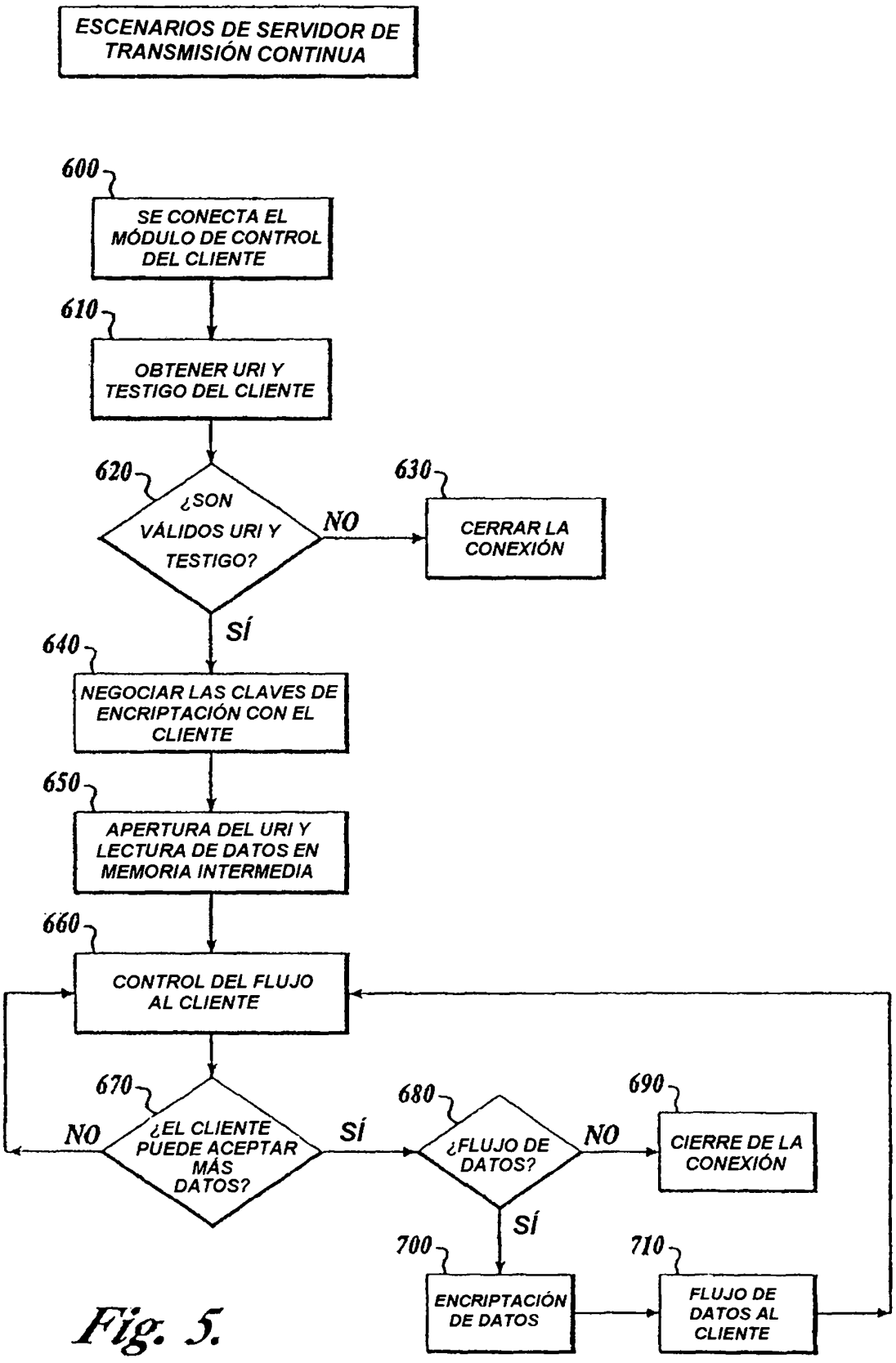
ESCENARIOS DE SERVIDOR DE TRANSMISIÓN CONTINUA
600
SE CONECTA EL MÓDULO DE CONTROL DEL CLIENTE
610
OBTENER URI Y TESTIGO DEL CLIENTE
620
¿SON VÁLIDOS URI Y TESTIGO?
NO
630
CERRAR LA CONEXIÓN
SÍ
640
NEGOCIAR LAS CLAVES DE ENCRIPTACIÓN CON EL CLIENTE
650
APERTURA DEL URI Y LECTURA DE DATOS EN MEMORIA INTERMEDIA
660
CONTROL DEL FLUJO AL CLIENTE
670
¿EL CLIENTE PUEDE ACEPTAR MÁS DATOS?
NO
SÍ
680
¿FLUJO DE DATOS?
NO
690
CIERRE DE LA CONEXIÓN
SÍ
700
ENCRIPTACIÓN DE DATOS
710
FLUJO DE DATOS AL CLIENTE

Fig. 5.

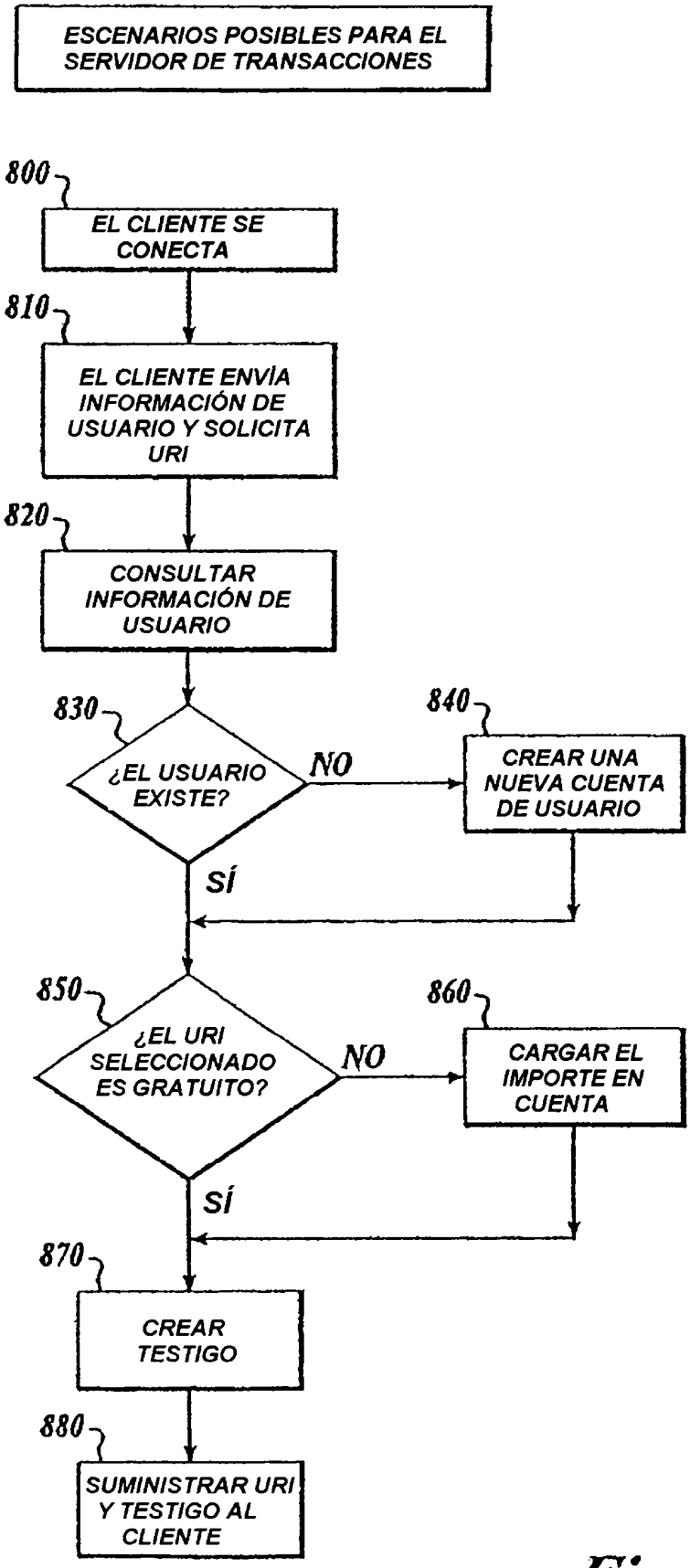
ESCENARIOS POSIBLES PARA EL SERVIDOR DE TRANSACCIONES
800
EL CLIENTE SE CONECTA
810
EL CLIENTE ENVÍA INFORMACIÓN DE USUARIO Y SOLICITA URI
820
CONSULTAR INFORMACIÓN DE USUARIO
830
¿EL USUARIO EXISTE?
NO
840
CREAR UNA NUEVA CUENTA DE USUARIO
SÍ
850
¿EL URI SELECCIONADO ES GRATUITO?
NO
860
CARGAR EL IMPORTE EN CUENTA
SÍ
870
CREAR TESTIGO
880
SUMINISTRAR URI Y TESTIGO AL CLIENTE

Fig. 6.

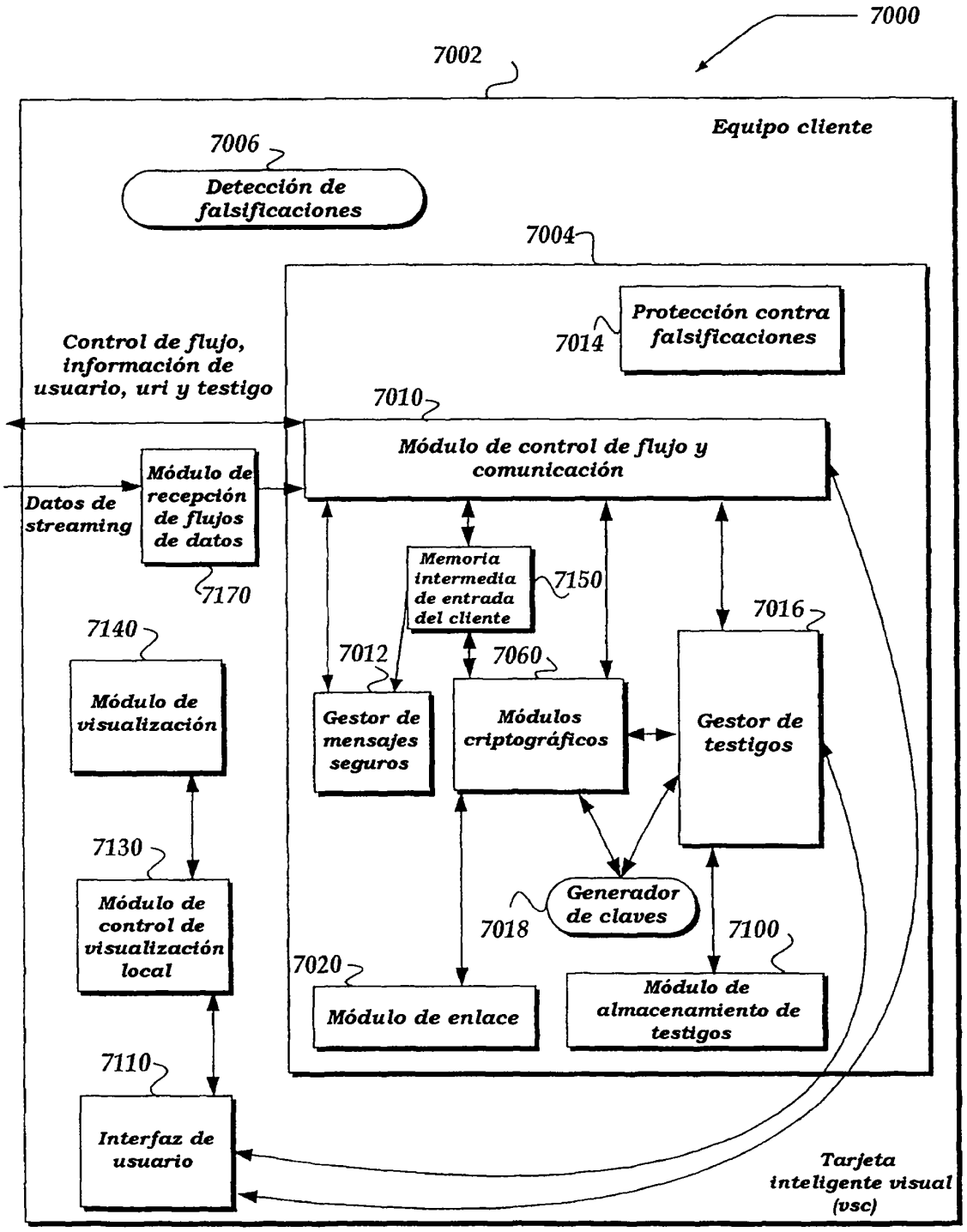
7000
7002
Equipo cliente
7006
Detección de falsificaciones
7004
Protección contra falsificaciones
7014
Control de flujo, información de usuario, uri y testigo
7010
Módulo de control de flujo y comunicación
Módulo de recepción de flujos de datos
Datos de streaming
7170
Memoria intermedia de entrada del cliente
7150
7016
7140
7012
7060
Módulo de visualización
Gestor de mensajes seguros
Módulos criptográficos
Gestor de testigos
7130
Módulo de control de visualización local
Generador de claves
7018
7100
7020
Módulo de enlace
Módulo de almacenamiento de testigos
7110
Interfaz de usuario
Tarjeta inteligente visual (vsc)

Fig. 7.