(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 286 268**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **02755084 .7**
(86) Fecha de presentación : **24.06.2002**
(87) Número de publicación de la solicitud: **1400090**
(87) Fecha de publicación de la solicitud: **24.03.2004**

(54) Título: **Procedimiento y dispositivo de aseguramiento de las comunicaciones en una red informática.**

(30) Prioridad: **27.06.2001 FR 01 08451**

(45) Fecha de publicación de la mención BOPI:
01.12.2007

(45) Fecha de la publicación del folleto de la patente:
01.12.2007

(73) Titular/es: **Amadeus S.A.S.**
485 route du Pin Montard, Sophia Antipolis
06410 Biot, FR

(72) Inventor/es: **Felix, Fabien**

(74) Agente: **Isern Jara, Jorge**

DESCRIPCIÓN

Procedimiento y dispositivo de aseguramiento de las comunicaciones en una red informática.

La presente invención se refiere a un procedimiento y a un dispositivo para el aseguramiento de las comunicaciones en el sistema informático. Un sistema de este tipo es conocido, por ejemplo, por el documento WO 03/003691 A1.

Un sistema de este tipo comprende, en general, una parte del servidor dotada como mínimo de un servidor central y una parte del cliente dotada como mínimo de una estación del cliente dispuesta, en general, de forma alejada de la parte del servidor y conectada a ésta por una red de comunicaciones.

Los clientes, tales como los empleados alejados del sistema informático central, pueden acceder al sistema por el rodeo de las estaciones de los clientes. Se identifican, de manera general, por un nombre de sesión asociado a los mismos.

La invención será especialmente aplicable para el aseguramiento de transmisiones informáticas utilizando el protocolo de comunicación TN 3270.

Este protocolo es utilizado por una parte importante de los ordenadores que corresponden al sistema llamado SNA (Systems Network Architecture, arquitectura en red de sistemas). El protocolo SNA define la forma en la que el programa del servidor central intercambia informaciones con el dispositivo de cliente. El protocolo SNA describe además los mensajes que son utilizados para los formatos de pantalla (tales como las solicitudes de regulación de la posición del indicador o el color de la pantalla), que se definen en forma de un flujo de datos en el formato 3270.

El aparato cliente que recibe el flujo de datos 3270 lo interpreta y genera el formato adecuado de pantalla según un juego de normas predeterminadas.

El protocolo de comunicación SNA se encontraba disponible en general en protocolos de nivel específico (tal como X25), pero no en protocolos de nivel más elevado, tal como TCP/IP (Transmission Control Protocol/Internet Protocol) (Protocolo de control de transmisión/protocolo de Internet) que permite a muchos sistemas con plataformas no homogéneas la comunicación entre sí.

Con el objeto de efectuar transferencias de flujo de datos 3270 en una red TCP/IP, la comunidad de Internet ha definido un protocolo denominado TN 3270E que está definido en los documentos siguientes: Request For Comment (RFC) 1576, 1647 y 2355 (Petición de comentario).

Las iniciales TN del protocolo significan Tel Net, estando especialmente definido el protocolo Tel Net en los documentos siguientes: Request For Comment (RFC) 854, 860 y 862.

La extensión numérica 3270 significa el formato del flujo de datos y la añadidura E significa extendida, tal como se define en el documento Request For Comment (RFC) 1647.

Para la descripción siguiente, se comprenderá por TN 3270 tanto la noción de protocolo TN 3270 como su extensión TN 3270E, teniendo en cuenta que el principio general de realización es exactamente el mismo para estos dos protocolos.

En el estado actual de la técnica, solamente se prevé un aseguramiento limitado y poco fiable en las comunicaciones informáticas utilizando una arquitectura, tal como se ha definido anteriormente, con una combinación del protocolo TN 3270 a través de la red informática pública del tipo de Internet.

En la actualidad, se atribuye únicamente un nombre de sesión a un cliente, siendo asociado este nombre de sesión a características almacenadas en una tabla de configuración del servidor, pero que presenta diferentes inconvenientes.

En primer lugar, el nombre de sesión del cliente es transmitido de manera legible a través de la red. Por lo tanto, es posible su pirateo.

Además, las características asociadas al nombre de sesión pueden comprender la dirección IP de la estación de cliente (dirección de localización asociada a una estación informática en una red de Internet según el protocolo Internet). Como consecuencia, si el cliente ha cambiado de dirección IP (por ejemplo, si se conecta a otro punto de la red), el servidor ya no le podrá reconocer autorizándole a acceder al sistema informático.

En resumen, se comprueba que los medios de actualización actualmente utilizados en el marco de estos sistemas son satisfactorios en una red privada, pero no son compatibles en una utilización en una red pública del tipo de Internet. En efecto, este tipo de aplicación necesita poder modificar dinámicamente algunos parámetros de conexión y, en especial, la dirección IP del cliente.

La presente invención permite solucionar los inconvenientes de las técnicas conocidas hasta el momento y presenta, para ello, un procedimiento y un dispositivo especialmente ventajosos.

Uno de los primeros objetivos de la invención consiste en utilizar un certificado numérico completo que permite la autentificación eficaz de cada cliente.

Esta creación de certificado numérico se efectúa de manera especialmente asegurada al nivel de la estación del cliente.

Además, se puede asociar al certificado numérico una transmisión asegurada de datos desde la estación del cliente hasta el servidor.

Estas ventajas, en cuanto al aseguramiento tanto de la utilización de acceso de los clientes como de las transmisiones a través de la red de comunicaciones, se producen realizando una implantación totalmente transparente para los componentes preexistentes del sistema informático. En particular, la presente invención puede ser instalada en forma de extensiones en sistemas ya existentes, sin que necesite, para ello, una modificación lógica o material de éstos, que puede generar numerosos inconvenientes prácticos.

Al proceder de este modo, la presente invención amplía las aplicaciones, en particular, las del protocolo TN 3270 puesto que permite recurrir a la red Internet clásica, en vez de limitarse a su utilización en redes privadas específicas.

Otros objetivos y ventajas aparecerán en el curso de la descripción siguiente, que presenta en detalle una forma de realización preferente de la invención que no es, sin embargo, limitativa.

La presente invención se refiere a un procedimiento de aseguramiento de las comunicaciones en un sistema informático, que comprende una parte de servidor dotada como mínimo de un servidor y una parte de cliente dotada como mínimo de una estación de cliente, mediante el cual un cliente puede acceder al sistema especificando un nombre de sesión, caracterizándose por las siguientes etapas:

- creación de un dispositivo de pasarela en la parte del servidor, en comunicación con el servidor,

- creación, en las proximidades físicas de cada estación de cliente, de un dispositivo de proximidad en comunicación con dicha estación de cliente y el dispositivo de pasarela,

- comunicación entre el servidor y la estación de cliente con intermedio de dispositivos de interfaz de proximidad y de pasarela,

- codificación de la totalidad o parte de la transmisión entre el dispositivo de pasarela y el dispositivo de interfaz de proximidad.

Este procedimiento se podrá presentar según las variantes que se indican a continuación:

- se memoriza en la estación de cliente y el dispositivo de interfaz de proximidad un certificado de autorización asociado a un nombre único de sesión de cliente,

- se presenta el certificado al servidor desde el dispositivo de interfaz de proximidad, con intermedio del dispositivo de pasarela, para verificación de la autorización de conexión del cliente,

- el certificado incluye el nombre de sesión del cliente,

- se memoriza el certificado en la estación de cliente y el dispositivo de interfaz de proximidad mediante:

- suministro a un instalador de un identificador de certificado y de un nombre de sesión facilitado por el servidor en la creación de la sesión en la estación de cliente por un organismo de certificación,

- instalación del certificado en la estación de cliente por telecarga del organismo de certificación bajo petición del instalador, condicionado a la presentación del identificativo de certificado e integrando el nombre de sesión del cliente por requerimiento del instalador.

- la codificación de los datos entre el dispositivo de pasarela y el dispositivo de interfaz de proximidad se efectúa por utilización de pares de llaves públicas y privadas,

- se utiliza el dispositivo de interfaz de proximidad en forma de extensión lógica implementada en la estación de cliente,

- el cliente toma su nombre de sesión a nivel de la estación de cliente en la configuración inicial de la aplicación de la estación de cliente,

- se verifica la identidad del nombre de sesión escogido y el que se ha incluido en el certificado

para verificar la autorización del cliente,

- se utiliza el protocolo de comunicación Telnet 3270,

- las comunicaciones en el sistema se efectúan por una red según la norma TCP/IP.

La invención se refiere igualmente a un sistema informático con comunicaciones aseguradas, que comprende una parte de servidor dotada como mínimo de un servidor y una parte de cliente dotada como mínimo de una estación de cliente, por el cual un cliente puede acceder al sistema escogiendo un nombre de sesión, apropiado para poner en práctica el procedimiento según la invención, caracterizado por el hecho de comportar:

- un dispositivo de pasarela en la parte del servidor, en comunicación con el servidor,

- un dispositivo de interfaz de proximidad en la proximidad física de cada estación de cliente, en comunicación con dicha estación de cliente y el dispositivo de pasarela,

- medios de codificación para las transmisiones entre el dispositivo de pasarela y el dispositivo de interfaz de proximidad.

Según una variante, los mensajes de transmisión entre el dispositivo de pasarela y el dispositivo de interfaz de proximidad comprenden un encabezamiento que integra datos de aseguramiento.

Los dibujos adjuntos tienen carácter de ejemplo y no son limitativos de la invención. Representan solamente una forma de realización de la invención y permitirán comprenderla con facilidad.

La figura 1 es una ilustración general de la arquitectura de un sistema informático, que utiliza una red de comunicación entre las estaciones de cliente y un servidor central.

La figura 2 es una representación esquemática de la invención.

La figura 3 muestra un formato de mensaje clásico, utilizando el protocolo TN 3270 a través de una red TCP/IP.

La figura 4 muestra un formato de mensaje característico de la invención.

La figura 5 muestra, de manera más precisa, las interacciones entre los elementos constitutivos del sistema utilizando la invención.

La descripción siguiente es un ejemplo preferente de la invención dentro del marco de la explotación de comunicaciones según el protocolo TN 3270 en una red de comunicaciones TCP/IP. Esta forma de realización preferente no es, sin embargo, limitativa de las aplicaciones de la invención.

La figura 1 muestra una ilustración de la arquitectura de una red en el formato TN 3270, tal como se conoce en la actualidad. Esta arquitectura comprende una serie de estaciones de cliente (4) que comunican a través de una red (7) con un servidor (3).

La figura 2 muestra una forma de realización de la invención y sus componentes característicos.

Se crea de inmediato, en la parte del servidor (1), un dispositivo de pasarela (5) preferentemente en forma de una extensión de programa del servidor (3). Esta extensión de programa no modifica, no obstante, la integridad de la configuración del servidor (3).

El dispositivo de pasarela (5) actúa como un intermediario entre la serie de estaciones de cliente (4) y el servidor (3) en sus comunicaciones a través de la red (7).

Por una parte, el dispositivo de pasarela (5) genera varias sesiones simultáneas TCP/IP con los programas soportados por las estaciones de cliente (4), y, por otra parte, varias sesiones simultáneas con el servidor (3).

De acuerdo con la invención, se crea igualmente un dispositivo de interfaz de proximidad (6) dispuesto en la parte del cliente, en las proximidades de cada una de las estaciones de cliente (4). En particular, se puede implantar el dispositivo de interfaz de proximidad (6) en forma de una extensión de programa de la estación de cliente (4). Esta extensión se efectúa conservando la integridad lógica de la estación de cliente (4).

De este modo, cuando tiene lugar una creación completa de la arquitectura de la red, es posible hacer específico el código fuente del programa de cliente TN 3270 (4) para integrar en el mismo las funcionalidades del dispositivo de interfaz de proximidad (6), con la finalidad de realizar un solo programa unitario.

El dispositivo de interfaz de proximidad (6) actúa como un intermediario entre las estaciones de cliente (4) y el dispositivo de pasarela (5). Como consecuencia, la combinación del dispositivo de pasarela (5) y el dispositivo de interfaz de proximidad (6) actúa como un verdadero conjunto intermedio de comunicación a través de la red (7).

Esta combinación permite asegurar las comunicaciones a través de la red (7) y, por adelantado, verificar las autorizaciones de los clientes.

Se describe a continuación, de manera más precisa, estas funcionalidades.

Para permitir la identificación segura de los clientes, se recurre de manera ventajosa al servicio de un organismo de certificación (9) tal como se ha esquematizado en la figura 2.

De manera conocida, el organismo (9) está constituido por un sitio de Internet al que se puede acceder para telecargar e instalar un certificado en cada estación de cliente (4), utilizando la invención. Se accede al servicio del organismo (9) una sola vez, para cada estación de cliente (4), cuando tiene lugar la instalación de la aplicación informática del cliente.

El objetivo esencial del certificado creado gracias al organismo (9) consiste en bloquear un nombre de sesión TN 3270 que podrá ser utilizado por el cliente. Un certificado numérico es una solución ideal para almacenar informaciones de identificación, puesto que los sistemas de navegación en Internet facilitan en general mecanismos que permiten proteger los certificados contra la copia desde un ordenador contra otro.

La presente invención utiliza otras funciones de los certificados y, en especial, las claves utilizadas para codificar y descodificar los datos intercambiados entre el dispositivo de pasarela (5) y el dispositivo de interfaz de proximidad (6).

Por otra parte, el certificado presenta una duración de vida predeterminada que le hace válido durante un período de tiempo determinado y que puede ser revocado en cualquier momento de manera centralizada.

El certificado numérico (10) creado según la invención consiste, en realidad, en un dato de acoplamiento de un mensaje electrónico utilizado para necesidades de seguridad. De manera conocida, los certificados numéricos son utilizados para verificar que la persona que envía mensajes es realmente la que dice ser, y para facilitar la persona que recibe el mensaje los medios para enviar una respuesta codificada.

Una persona que desee enviar mensajes codificados pide a un organismo de certificación la atribución de un certificado numérico o implementa entonces por sí misma el servicio, declarándose a sí misma autoridad de certificación.

El organismo de certificación (9) es un tercero de confianza, tal como una empresa profesional en este tipo de servicios, que facilita certificados numéricos para crear firmas numéricas y pares de claves públicas y privadas. El papel del organismo de certificación (9), en el procedimiento según la invención, es el de garantizar que el cliente que presenta un certificado único es de forma real el que dice ser. De manera general, esto significa que el organismo de certificación (9) tiene acuerdos con instituciones financieras, tales como una empresa de crédito, que le facilita informaciones para confirmar la identidad de cada individuo.

El organismo de certificación (9) suministra un certificado numérico codificado, que contiene diversas informaciones de identificación del cliente así como una clave pública. El organismo de certificación (9) establece su propia clave pública accesible por cualquier medio de comunicación y, especialmente, por la acción de su lugar de Internet.

La persona que reciba un mensaje codificado recupera y utiliza la clave pública del organismo de certificación (9) para decodificar el certificado numérico asociado al mensaje codificado. Verifica, de este modo, que el certificado ha sido suministrado correctamente por el organismo de certificación (9) y obtiene la clave pública del remitente del mensaje, así como informaciones de identificación contenidas en el certificado. Con estas informaciones, la persona que recibe el mensaje puede enviar entonces una respuesta codificada.

La presente invención utiliza preferentemente este sistema de claves públicas para la codificación y decodificación de las transmisiones. En este ámbito, se requieren dos claves para permitir a las partes intercambiar informaciones de manera asegurada: una clave pública y una clave privada. Un ejemplo de realización se presenta en la figura 5 para la utilización de dichos pares de claves públicas-privadas.

Una de las claves del par de claves es utilizada para codificar el mensaje (clave pública), mientras que la otra es utilizada para descodificarlo (clave privada). Cuando el dispositivo de interfaz de proximidad (6) quiere dirigir un mensaje codificado al dispositivo de pasarela (5), lo codifica utilizando la clave pública y el dispositivo de pasarela (5), que es el único poseedor de la clave privada correspondiente del par de claves, es el único dispositivo que lo puede descodificar.

Si bien las claves públicas y privadas de un par están matemáticamente correlacionadas, en la práctica, es imposible deducir una de otra. Como consecuencia, el carácter público de una de las claves no dificulta el aseguramiento de la codificación.

En especial, se podrá utilizar, para la realización del certificado (10) según la invención, el formato muy extendido para los certificados numéricos según la norma ITU-T X.509.

Este formato comprende los campos siguientes: versión, número de serie, identificativo de algoritmos de firma, nombre del suministrador del certificado, período de validez, nombre del usuario, información referente a la clave pública del usuario, identificador único del suministrador, identificador único del usuario, extensiones, firma sobre los campos precedentes. El certificado está firmado por el suministrador para autentificar la relación existente entre el nombre del usuario y la clave pública del usuario.

La presente invención utiliza un campo de texto libre en este certificado. En efecto, el campo "nombre del usuario" es utilizado para almacenar el nombre de sesión del cliente que puede ser utilizado en la estación de cliente que ha efectuado su telecarga.

Con objetivos de seguridad, el organismo de certificación (9) marca el certificado (10) como no exportable, es decir que no puede ser reinstalado en otra estación de cliente una vez que se ha efectuado la etapa de instalación.

El organismo de certificación (9), que puede ser también la sociedad que utiliza la invención, utiliza un programa que se puede basar en un servidor informático WEB o sobre un servidor específico. Le corresponde la carga de acceder a una tabla de correspondencia que va a conectar los nombres de sesión TN 3270 con un identificativo de certificado. Cada vez que un nuevo nombre de sesión de cliente es atribuido mediante el servidor (3) para un nuevo cliente, se añade una nueva entrada a la tabla de correspondencia por los administradores del sistema. El identificativo del certificado es un número aleatorio único para cada nombre de sesión.

Se describen, a continuación, las etapas de la instalación del certificado en una estación de cliente (4) en una forma preferente de realización.

En una primera etapa, el identificativo de certificado y también el nombre de sesión son dirigidos a la persona que está a cargo de instalar el certificado (10) en la estación de cliente (4). Se recuerda que, de manera ventajosa, la estación de cliente (4) recibe los medios lógicos igualmente necesarios para las funcionalidades del dispositivo de interfaz de proximidad. Una única implantación material del certificado (10) queda entonces efectiva simultáneamente en la estación de cliente (4) en sus funciones generales y para el dispositivo de interfaz de proximidad (6).

El instalador, que, de este modo, tiene conocimiento del identificador de certificado y del nombre de sesión, se conecta a nivel de la estación de cliente (4) al servicio del organismo de certificación (9) por medio de la red de Internet. Este último solicita al instalador que tome el identificativo de certificado. El instalador efectúa esta elección y el identificador de certificado es devuelto al organismo de certificación (9), que verificará en la tabla de correspondencia a qué nombre de sesión está relacionado este identificador. El organismo de certificación (9) dirigirá entonces una página WEB a la estación de cliente (4), permitiéndole instalar el certificado que incluye el nombre de sesión correcto en el campo "nombre del usuario" del certificado (10).

La figura 5 muestra las interacciones existentes entre el instalador, la estación de cliente (4) y el organismo de certificación (9).

Una vez que la instalación de certificado (10) se ha realizado satisfactoriamente, el servicio del organismo de certificación (9) ya no es utilizado por el cliente.

Tal como se ha indicado en lo anterior, el dispositivo de interfaz de proximidad (6) es instalado ventajosamente en la estación de cliente (4) y funciona en paralelo con la aplicación de cliente.

El dispositivo (6) autentifica al cliente en su entrada en la sesión, autorizando la negociación del nombre de sesión únicamente para el nombre de sesión instalado en la estación del cliente (4), en especial según el procedimiento de certificado (10) que se ha citado anteriormente.

Por otra parte, el dispositivo de interfaz de proximidad (6) codifica los datos que son intercambiados con el servidor (3) por intermedio del dispositivo de pasarela (5).

Por lo tanto, el dispositivo de interfaz de proximidad (6) en forma de programa actúa como un cliente TCP/IP para el dispositivo de pasarela (5) y como servidor local TCP/IP para aceptar o rechazar la conexión de un cliente.

La aplicación de cliente TN 3270 (4) entra en conexión con el dispositivo de interfaz de proximidad (6) y, por su parte, se conecta al dispositivo de pasarela (5).

Gracias a la invención, el programa de aplicación TN 3270 ejecutado sobre la estación de cliente (4) puede seguir siendo el programa estándar inicial utilizado por el cliente hasta aquel momento.

Se describirán, a continuación, las etapas de establecimiento de la comunicación para un cliente hacia el servidor (3), hasta que estas dos entidades estén preparadas para intercambiar datos.

En un primer tiempo, la estación de cliente se conecta al dispositivo de interfaz de proximidad (6).

El dispositivo de interfaz de proximidad (6) acepta la conexión del cliente y se conecta al dispositivo de pasarela (5).

Cuando el dispositivo de pasarela (5) acepta la conexión del dispositivo de interfaz de proximidad (6), empieza un proceso interno de seguridad que depende de la implementación efectuada en la instalación. A título de ejemplo preferente, es posible, en este momento, presentar el certificado (10) del servidor (3) para verificar su validez. Este mensaje de presentación de certificado tiene ventajosamente el formato específico que se describe más adelante en relación con la figura 4. Si el certificado (10) no es válido, el dispositivo de pasarela (5) rechaza la conexión y desconecta inmediatamente el dispositivo de interfaz de proximidad (6).

La utilización a este nivel del certificado (10) como clave numérica es muy ventajosa puesto que el dispositivo de pasarela (5) puede utilizar varios criterios para la verificación de la autorización de conexión, a saber:

- la autoridad que ha suministrado el certificado (organismo de certificación (9)) deber ser válida (para evitar que personas actuando de forma no autorizada creen un falso certificado que contenga el nombre adecuado de la sesión, pero no firmado por la autoridad adecuada de certificación),

- la fecha de validez del certificado (10) no debe haber expirado,

- el certificado (10) no debe haber sido revocado (si el servidor (3) genera una lista negra de los certificados revocados, incluso si el usuario tiene un nombre de sesión válido, no se podrá conectar).

Un mensaje de estado de certificado (indicando si el certificado presentado es válido) es devuelto al dispositivo de interfaz de proximidad (6) de manera ventajosa con el formato de mensaje descrito más adelante en relación con la figura 4.

Si el dispositivo de pasarela (5) ha validado el certificado (10), se conecta al servidor (3) igual que en una estación de cliente (4) clásica, según el estado de la técnica.

Si el servidor (3) acepta esta conexión, empieza una negociación de protocolo enviando un flujo de datos al dispositivo de pasarela (5).

Este último codifica el flujo de datos y lo envía al dispositivo de proximidad de interfaz (6) (ventajosamente en forma de un mensaje de tipo “datos codificados” cuyo formato se describe más adelante en relación con la figura 4). El dispositivo de pasarela (5) y el dispositivo de proximidad (6) utilizan este formato que lo decodifica y dirige los datos a la estación de cliente (4) utilizando la conexión establecida previamente.

En este instante, la estación de cliente (4) ha recibido el mensaje inicial del servidor (3). Puede responder al mismo.

El dispositivo de interfaz de proximidad (6) recibe este mensaje de respuesta y lo codifica para enviarlo, a continuación, al dispositivo de pasarela (5) que lo decodifica y lo envía a su vez al servidor (3).

El servidor (3) analiza esta respuesta y solicita al cliente información suplementaria, a saber, tipo de material que quiere utilizar, así como el nombre de la sesión.

Igual que en el caso anterior, esta solicitud complementaria es transmitida a través del dispositivo de pasarela (5) y después del dispositivo de interfaz (6) por una etapa de codificación y de decodificación. La solicitud del servidor (3) es recibida finalmente por la estación de cliente (4).

La estación de cliente (4) responde a este mensaje enviando nuevamente un mensaje al dispositivo de interfaz de proximidad (6), respondiendo a la interrelación del servidor (3), mencionando el tipo de aparato y el nombre de sesión que el cliente ha escogido.

El dispositivo de interfaz de proximidad (6) detecta que este mensaje de respuesta contiene la solicitud de utilización de un nombre de sesión de cliente específico. Por este hecho, a efectos de control, se verifica, en este instante, que el nombre de sesión específico configurado en la aplicación de cliente TN 3270 corresponde con el que se encuentra presenta en uno de los certificados (10) instalados en la estación de cliente (4).

Si el nombre de sesión aparece en un certificado (10), el cliente está autorizado a continuar la comunicación y el dispositivo de interfaz de proximidad acepta pasar a la etapa siguiente.

Si el nombre de sesión no corresponde a ningún certificado válido (10), el dispositivo de interfaz de proximidad (6) rechaza la solicitud del cliente.

Cierra igualmente las conexiones establecidas con la estación de cliente (4) y el dispositivo de pasarela (5). De forma consecutiva, el dispositivo de pasarela (5) cierra la sesión TCP/IP establecida para este cliente con el servidor (3).

En lugar de abandonar el conjunto de este proceso, el dispositivo de interfaz de proximidad (6) puede también cambiar el nombre de sesión no válido y un nombre de sesión que retira un certificado (10) válido, y continuar la comunicación.

Cuando se ha llevado a cabo esta verificación del nombre de sesión y sus consecuencias, el dispositivo de interfaz de proximidad (6) codifica el mensaje de respuesta del cliente utilizando la clave pública del dispositivo de pasarela (5) y lo envía a éste. El dispositivo de pasarela (5) descodifica el mensaje con su clave privada y lo envía, a su vez, al servidor (3).

Estas etapas de utilización de clave pública y de clave privada se han mostrado en especial en la figura 5.

En este momento, el servidor (3) recibe el nombre de sesión que debe ser utilizado para el cliente que se conecta y puede asociar al mismo la configuración correcta de funcionamiento.

Las etapas siguientes de negociación, según el protocolo TN 3270, pueden continuar utilizando el mismo método de transmisión.

De manera preferente, a cada comunicación, el dispositivo de interfaz de proximidad (6) y el dispositivo de pasarela (5) actúan como elementos de codificación y de decodificación, y como direccionadores entre los clientes y el servidor (3).

En lo que respecta al formato de las transmisiones entre el dispositivo de interfaz de proximidad (6) y el dispositivo de pasarela (5), la figura 3 muestra un ejemplo general del formato de los mensajes según el estado de la técnica, utilizando el protocolo TN 3270 en una red de comunicaciones TCP/IP.

La figura 4 muestra, por su parte, un formato característico de mensaje utilizado según la invención. En efecto, los datos TCP presentes en el mensaje son descompuestos, según esta característica, en un encabezamiento y en una parte de mensaje codificado TN 3270.

El encabezamiento en cuestión depende del tipo de mensaje dirigido y, en especial, de la etapa de intercambio en la iniciación de la conexión al servidor, tal como se ha descrito en lo anterior.

En particular, los datos de aseguramiento serán transmitidos ventajosamente a nivel de este encabezamiento. Por lo tanto, el encabezamiento se podrá presentar según el formato que se definirá sucesivamente para el envío del mensaje de presentación del certificado (10) desde el dispositivo de interfaz de proximidad (6) hacia el dispositivo de pasarela (5), el mensaje consecutivo de estado de certificado dirigido desde el dispositivo de pasarela (5) hacia el dispositivo de interfaz de proximidad (6), y después para los mensajes de tipo que comprenden los datos codificados.

	Desplazamiento 1	1	2...5	6	7...n
	Firma del mensaje	Firma del mensaje	Dimensiones del mensaje	Tipo de mensaje	Datos funciones del tipo de aseguramiento
Presentación de certificado	0X00	0X00	dimensiones	0X13	Certificado
Estado de certificado	0X00	0X00	dimensiones	0X13	Código de respuesta
Datos codificados	0X00	0X00	dimensiones	0X02	Datos codificados TN 3270

La utilización de este encabezamiento específico en el formato de los mensajes trasmitidos entre los dispositivos (5) y (6) asegura una comunicación asegurada durante la fase de negociación para la autorización y también durante la fase posterior de transmisión de datos.

Referencias

(1) Parte de servidor

(2) Parte de cliente

(3) Servidor

(4) Estación del cliente

(5) Dispositivo de pasarela

(6) Dispositivo de interfaz de proximidad

(7) Red

(8) Cliente

(9) Organismo de certificación

(10) Certificado.

REIVINDICACIONES

1. Procedimiento de aseguramiento de comunicaciones en un sistema informático, que comprende una parte de servidor (1) dotada como mínimo de un servidor (3) y una parte de cliente (2) dotada como mínimo de una estación de cliente (4), mediante la que un cliente (8) puede acceder al sistema especificando el nombre de la sesión, que comprende las siguientes etapas:

- creación de un dispositivo de pasarela (5) en la parte del servidor (1), en comunicación con el servidor (3),

- creación, en las proximidades físicas de cada estación de cliente (4), de un dispositivo de proximidad (6) en comunicación con dicha estación de cliente (4) y el dispositivo de pasarela (5),

- comunicación entre el servidor (3) y la estación de cliente (4) con intermedio de los dispositivos de interfaz de proximidad (6) y de pasarela (5),

- codificación de la totalidad o una parte de la transmisión entre el dispositivo de pasarela (5) y el dispositivo de interfaz de proximidad (6).

2. Procedimiento, según la reivindicación 1, **caracterizado** porque

- se memoriza en la estación de cliente (4) y el dispositivo de interfaz de proximidad (6) un certificado (10) de autorización asociado a un nombre único de sesión de cliente,

- se presenta el certificado (10) al servidor (3) desde el dispositivo de interfaz de proximidad (6), con intermedio del dispositivo de pasarela (5), para verificación de la autorización de conexión del cliente (8).

3. Procedimiento, según la reivindicación 2, **caracterizado** porque el certificado (10) incluye el nombre de sesión del cliente (8).

4. Procedimiento, según la reivindicación 3, **caracterizado** porque se memoriza el certificado (10) en la estación de cliente (4) y el dispositivo de interfaz de proximidad (6) por:

- suministro a un instalador de un identificador de certificado y un nombre de sesión facilitado por el servidor, cuando tiene lugar la creación de la sesión en la estación de cliente (4),

- instalación del certificado (10) en la instalación de cliente (4) por telecarga del organismo de certificación (9), a petición del instalador condicionada a la presentación del identificador de certificado e integrando en el mismo el nombre de sesión del cliente por elección del instalador.

5. Procedimiento, según cualquiera de las reivindicaciones 1 a 4, **caracterizado** porque la codificación de los datos entre el dispositivo de pasarela (5) y el dispositivo de interfaz de proximidad (6) se efectúa por utilización de pares de claves públicas y privadas.

6. Procedimiento, según cualquiera de las reivindicaciones 1 a 5, **caracterizado** porque se utiliza un dispositivo de interfaz de proximidad (6) en forma de extensión de programación implementada en la estación de cliente (4).

7. Procedimiento, según la reivindicación 3 ó 4, **caracterizado** porque:

- el cliente (8) recoge su nombre de sesión a nivel de la estación de cliente (4) en el momento de la configuración inicial de la aplicación de la estación de cliente (4),

- se verifica la identidad del nombre de sesión escogido y el incluido en el certificado (10),

para verificar la autorización del cliente (8).

8. Procedimiento, según cualquiera de las reivindicaciones 1 a 7, **caracterizado** porque se utiliza el protocolo de comunicación Telnet 3270.

9. Procedimiento, según cualquiera de las reivindicaciones 1 a 8, **caracterizado** porque las comunicaciones en el sistema se efectúan por una red según la norma TCP/IP.

10. Sistema informático de comunicaciones aseguradas, que comprende una parte de servidor (1) dotada como mínimo de un servidor (3) y una parte de cliente (2) dotada como mínimo de una estación de cliente (4), mediante el cual un cliente (8) puede acceder al sistema escogiendo un nombre de sesión, apropiado para poner en práctica el procedimiento según cualquiera de las reivindicaciones 1 a 9, comportando:

- un dispositivo de pasarela (5) en la parte de servidor (1), en comunicación con el servidor (3),

- un dispositivo de interfaz de proximidad (6) en las proximidades físicas de cada estación de cliente (4), en comunicación con dicha estación de cliente (4) y el dispositivo de pasarela (5),

- medios de codificación para las transmisiones entre el dispositivo de pasarela (5) y el dispositivo de interfaz de proximidad (6).

11. Sistema, según la reivindicación 10, **caracterizado** porque los mensajes de transmisión entre el dispositivo de pasarela (5) y el dispositivo de interfaz de proximidad (6) comprenden un encabezamiento integrando datos de aseguramiento.

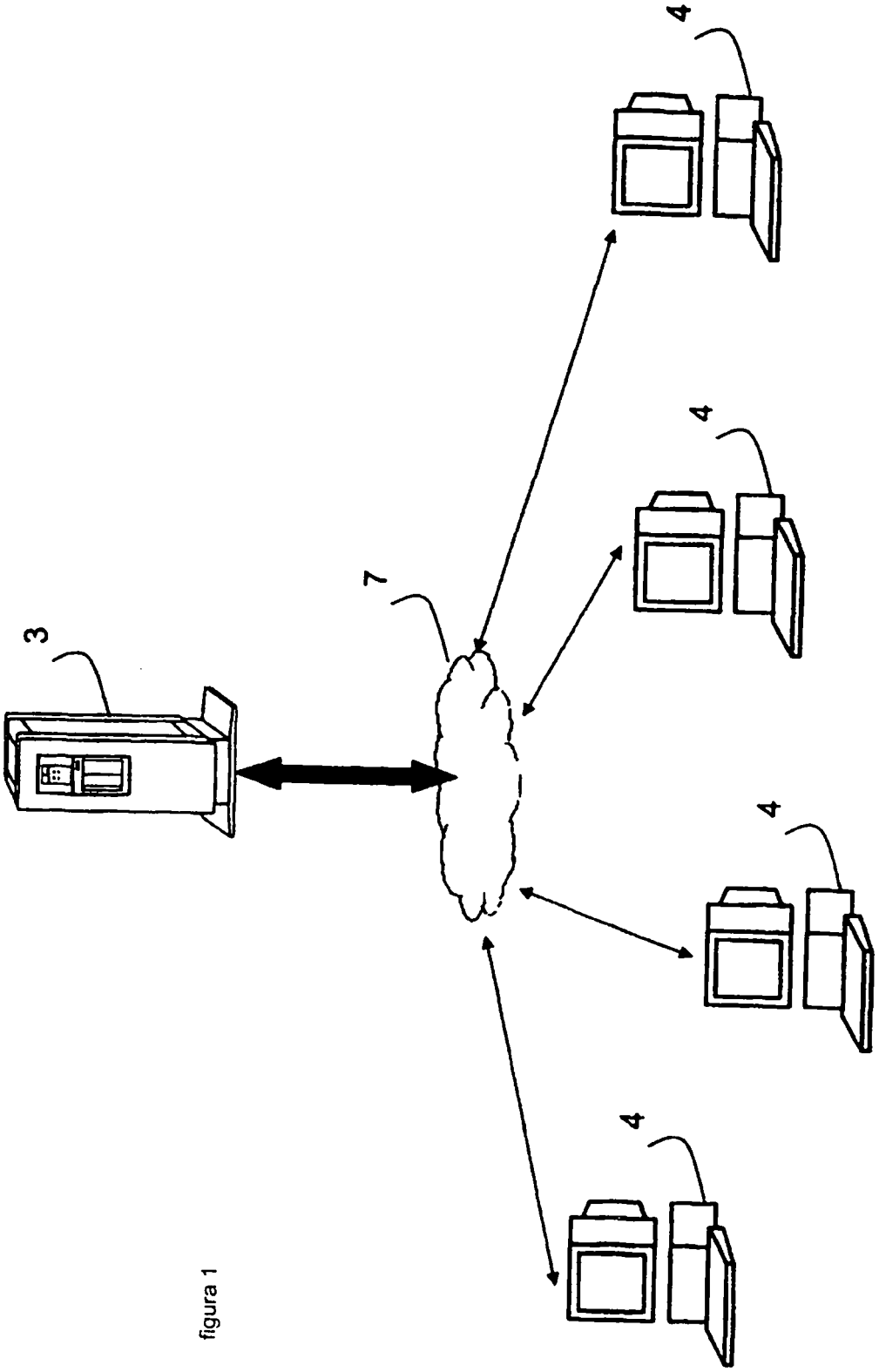


figura 1

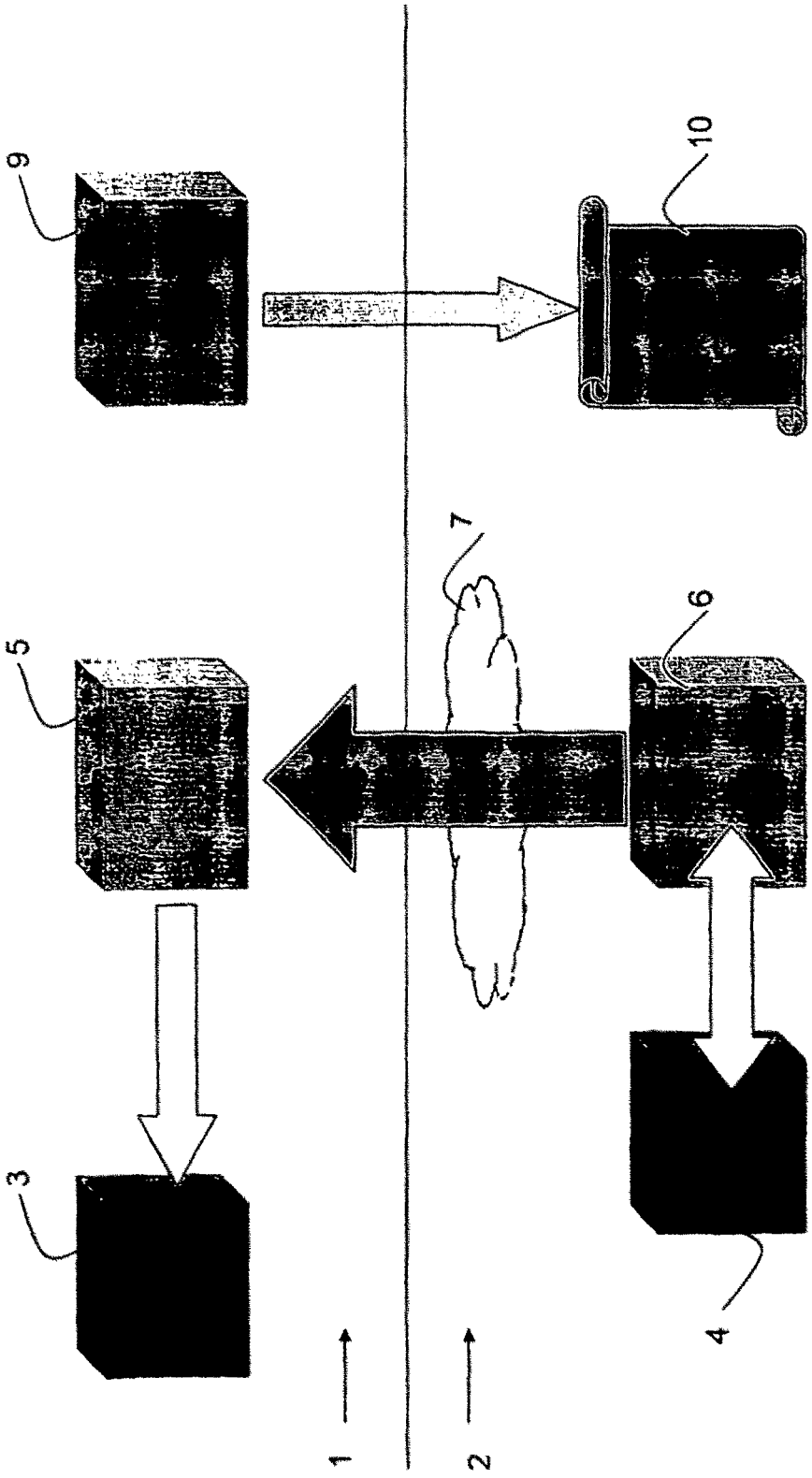


Figura 2

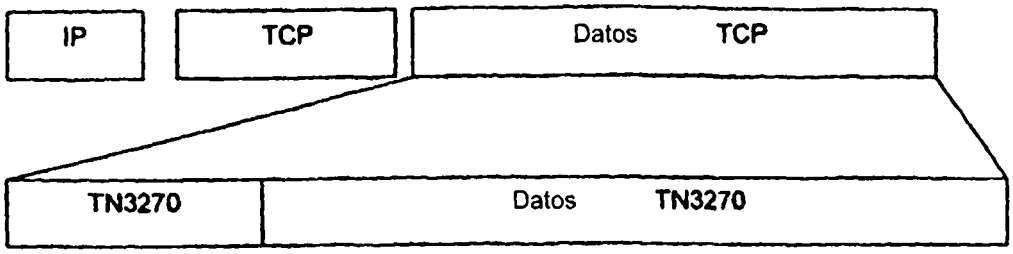


FIGURA 3

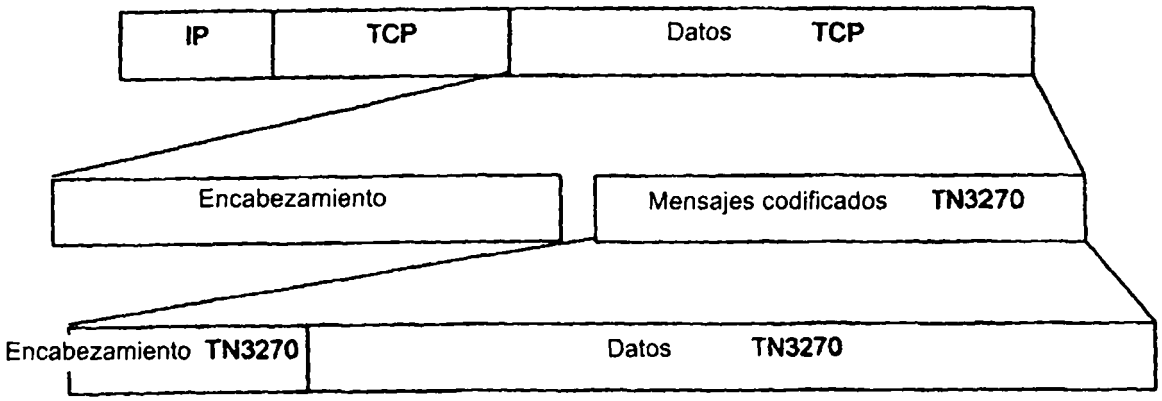
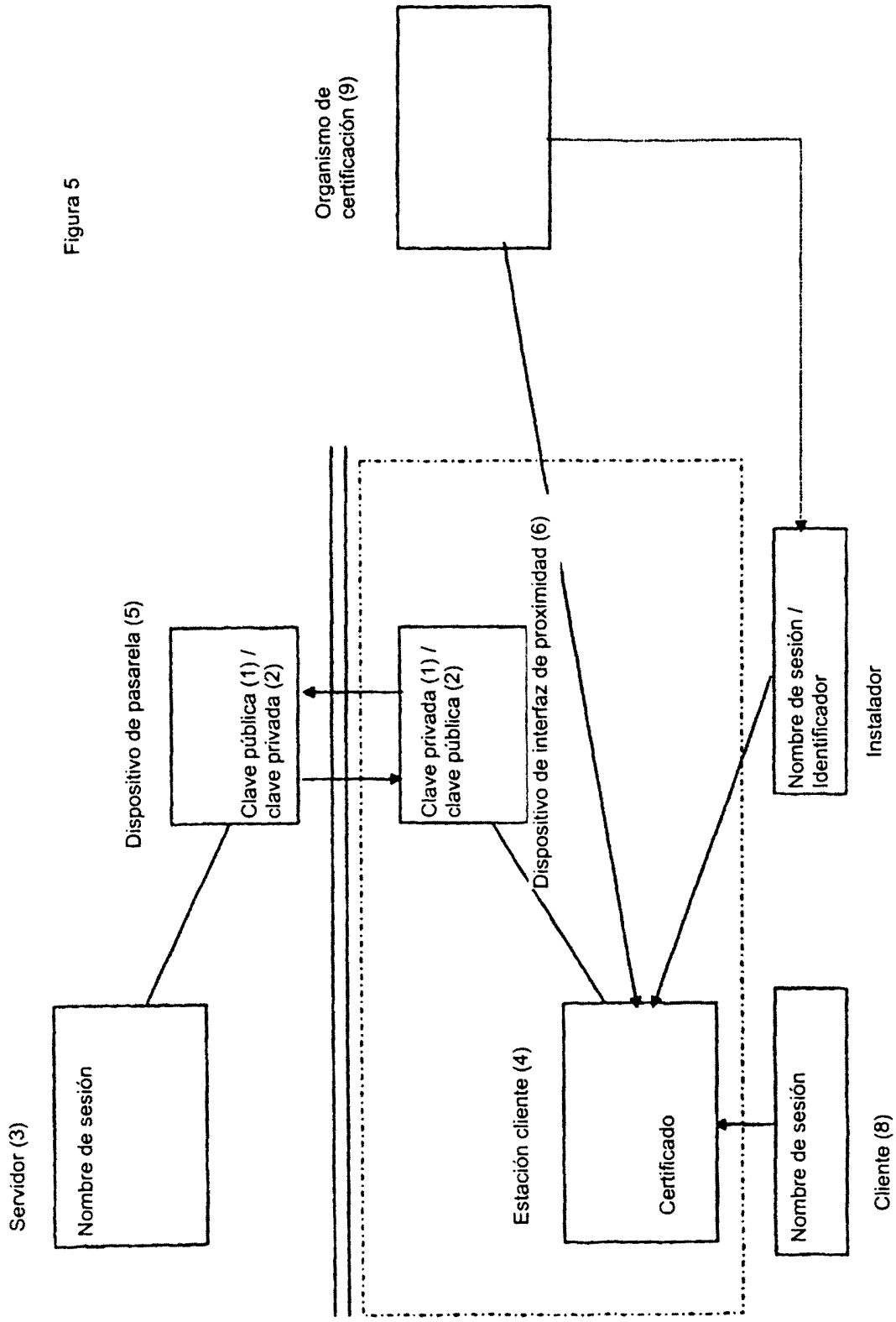


FIGURA 4

Figura 5


Organismo de certificación (9)
Dispositivo de pasarela (5)
Clave pública (1) / clave privada (2)
Clave privada (1) / clave pública (2)
Dispositivo de interfaz de proximidad (6)
Nombre de sesión / Identificador
Instalador
Servidor (3)
Nombre de sesión
Estación cliente (4)
Certificado
Nombre de sesión
Cliente (8)