

I.E.



Industria y Comercio

SUPERINTENDENCIA

Delegatura de propiedad Industrial

División de Nuevas Creaciones

PCT

SOLICITUD

PATENTE DE INVENCION

06-60188

21. EXPEDIENTE No.

54. TÍTULO

SISTEMA DE AUTENTICACIONES DE
COMPUTADORAS CONECTADAS EN RED

51. CLASIFICACIÓN INTERNACIONAL

H04L 29/06; 9/32

71. SOLICITANTE

WACHOVIA CORPORATION

DOMICILIO

CHARLOTTE, NORTH CAROLINA, EEUU

14. APODERADO

CARLOS ORLANDO MAYA RODRIGUEZ

22. BOGOTÁ, D. C.,

21 de Junio, 2006

Industria y Comercio
SUPERINTENDENCIA

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
Rad: 06-060188- -00000-0000
Fec: 2005-05-21 18:01:15 Dep. 2020 NUECREACIONES
Tra: 11 PATENTE/II
Eve: 379 FASENACIONAL/II
Act: 411 PRESENTACION Folio: 79

FORMULARIO UNICO DE SOLICITUD DE PATENTE
PCT
ENTRADA EN FASE NACIONAL

1. SOLICITUD DE:

☒ Patente de Invención

☐ Patente de Modelo de Utilidad

☐ Capítulo I

☒ Capítulo II

2.
SOLICITANTE
(/1)

Nombre:

WACHOVIA CORPORATION

Dirección 201 South College Street, Charlotte,
North Carolina

Nacionalidad o Domicilio:
North Carolina 28288, EE.UU.

Lugar de Constitución: CAROLINA DEL NORTE

Teléfono

Fax:

E-mail:

IDENTIFICACION

C.C. ☐

NIT ☐

C.E. ☐

Otro ☐

Cual _____

Número: _____

3.
REPRESENTANTE
O APODERADO

Nombre: CARLOS ORLANDO MAYA
RODRIGUEZ

Dirección: Cr. 13 A No 28-38, Mz 2
Bufete 245. Parque Central Bavaria

Teléfono 3419841 Fax: 3368592

E-mail: tmcarlos@etb.net.co

IDENTIFICACION

C.C. ☐

NIT ☐

C.E. ☐

Otro ☐

Cual _____

Número: 17.117.818 TP: 17.402

4.
INVENTOR(ES)
(72)

Nombres: 1.- KELLY, EDWARD R.
2.- HOWSER, CHRISTOPHER WAYNE

OTROS INVENTORES EN HOJA ANEXA

Dirección: 1.- 1289 Centennial Drive, Rock Hill, SC 29732, EE.UU
2.- 1842 Park Grove Place NW, Concord, NC 28027, EE.UU

Nacionalidad o Domicilio: 1.- Ciudadano de EE.UU
2.- Ciudadano de EE.UU

5. PCT (86)

Solicitud internacional No. PCT/US2004/043755

Fecha: 22/12/2004

Publicación internacional No. WO 2005/062989 A2

Fecha: 14/07/2005

6. Título (54)

SISTEMA DE AUTENTICACION PARA APLICACIONES DE COMPUTADORAS CONECTADAS
EN RED

7. Clasificación Internacional (51)

8. Prioridad

Si ☒ No ☐

(33) País de Origen

EE.UU

(32) Fecha

23/12/2003

(31) Número de Solicitud

60/531,898

9. Comprobante de pago No. 06-47,269 Fecha JUNIO 21/2006

CONTINUACION DE INVENTORES**3.- SAVAGE, JONATHAN FRANCIS.**

Domicilio: 10001 Lampkin Way, Charlotte, NC 28269, EE.UU.

Ciudadano de Gran Bretaña.

4.- ZHENG, YULIANG.

Domicilio: 3122 Bridle Brook Way, Charlotte, NC 28270, EE.UU.

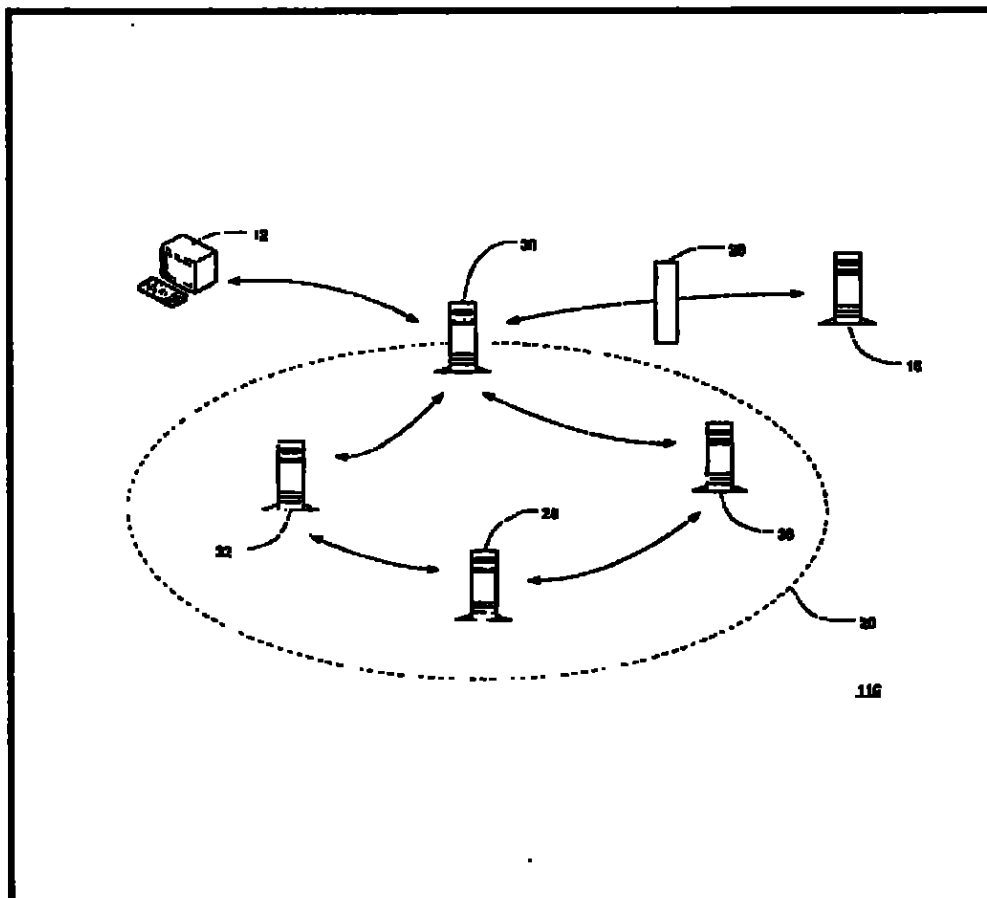
Ciudadano de Australia.

10.

Anexos

- ☒ Comprobante de pago de la tasa de presentación de la solicitud
- ☐ Documento que acredite la existencia y representación legal cuando el solicitante sea persona jurídica
- ☐ Poderes, si fuere el caso
- ☐ Documento de cesión del inventor al solicitante o a su causante
- ☐ Declaraciones
- ☐ Copia de la solicitud Internacional (Resumen, descripción, reivindicaciones, dibujos)
- ☐ Traducción de la solicitud internacional al castellano (Resumen, descripción, reivindicaciones, dibujos)
- ☐ Copia del examen preliminar internacional efectuado por la Autoridad Internacional de Examen Preliminar (IPEA)
- ☐ Traducción del examen preliminar internacional efectuado por la IPEA
- ☐ De ser el caso, copia del contrato de acceso
- ☐ De ser el caso, documento que acredite la licencia o autorización de uso de conocimientos tradicionales de las comunidades indígenas.
- ☐ De ser el caso, certificado de depósito del material biológico
- ☒ Arte final 12 x 12
- ☐ De ser el caso, información sobre otras solicitudes de patente o títulos obtenidos en el extranjero por el mismo titular o su causante, relacionadas parcial o totalmente con la invención de esta solicitud.
- ☐ De ser el caso, modificaciones efectuadas a la solicitud internacional
- ☒ Otros (FOTOCOPIA DE LA PUBLICACION INTERNACIONAL)

11. FIGURA CARACTERISTICA



12. Solicito la concesión de la patente,

NOMBRE: CARLOS ORLANDO MAYA RODRIGUEZFIRMA: *C. O. Maya*

C.C 17.117.818 TP 17.402

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
Rad: 06-060188-00000-0000
Fec: 2006-06-21 15:01:15 Dep. 2000 NUECREACIONEE
Tib. 11 PATENTEYII
Ere: 379 FASENACIONALI
Act 411 PRESENTACION Folios: 79

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800176089-2

RECIBO OFICIAL DE CAJA : 06 - 47,269
FECHA : JUNIO 21 DE 2006

***** CONSIGNACION *****

DEPOSITANTE	TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PGO	Vr. PAGO
CARLOS TANAYO Y ASOCIADOS	CONSIGNACION	BANCO POPULAR	050-00110-6	48895577	21/06/2006	558,000.00

***** CONCEPTO *****

CANT.	RENTISTICO	CONCEPTO	TOTAL CONCEPTO
1	50005-01-01	SOLICITUDES	
1		TRAMITES DE SOL. DE PATENTE DE IN	463,000.00
		TOTAL :	\$ 463,000.00

SON: CUATROCIENTOS SESENTA Y TRES MIL PESOS

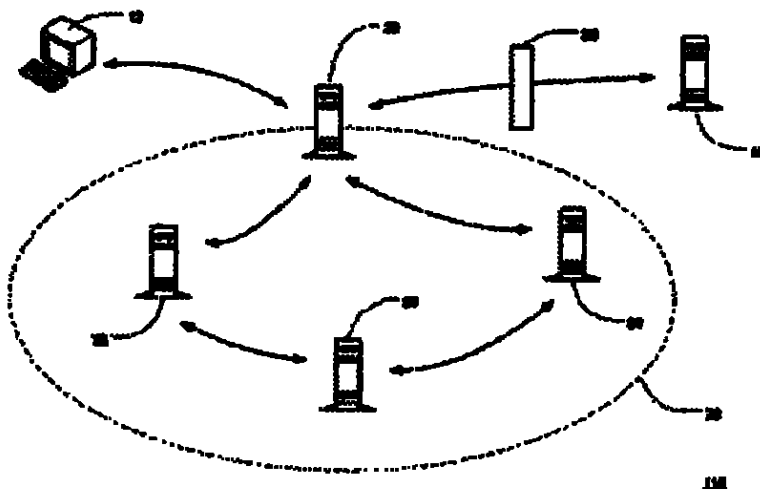


RESPONSABLE : _____

RECIBO DE CAJA APLICADO AL EXPEDIENTE No. _____

 Industria y Comercio SUPERINTENDENCIA		SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DIVISION DE NUEVAS CREACIONES EXTRACTO PARA PUBLICACIÓN SOLICITUD DE PATENTE DE INVENCION PCT	
(21) N° de solicitud (22) Fecha de solicitud 21-06-2006 (30) Prioridad SI (31) No. Prioridad 60/631.695 (32) Fecha 23/12/2003 (33) País E.U		(51) Int Cl (71) Solicitante(s) WACHOVIA CORPORATION (72) Inventor(es) 1.- KELLY, EDWARD R 2.- HOWSER, CHRISTOPHER WAYNE 3.- SAVAGE, JONATHAN FRANCIS 4.- ZHENG, YULIANG. (74) Apoderado: CARLOS ORLANDO MAYA RODRIGUEZ	
(85) Fecha límite inicio fase nacional: (86) Datos relativos a la presentación de la solicitud PCT Fecha de presentación de la solicitud: Fecha 09/12/2003 No. de solicitud PCT/US2004/043755		(87) Publicación Internacional Fecha: Fecha 14/07/2005 N° publicación: WO 2005/062806 A2	
(54) Título: SISTEMA DE AUTENTICACION PARA APLICACIONES DE COMPUTADORAS CONECTADAS EN RED			

Reivindicación(es):



Un método de autenticar a un usuario con un servidor de autenticación en un sistema de computadoras conectadas en red, el método comprende:

- (a) presentar credenciales de usuario por un usuario a un servidor protector de compuerta;
- (b) proporcionar las credenciales de usuario por un servidor protector de compuerta a un servidor de autenticación;
- (c) autenticar al usuario por el servidor de autenticación;
- (d) crear una señal de autenticación por el servidor de autenticación al ocurrir la autenticación del usuario; y
- (e) transmitir la señal de autenticación por el servidor de autenticación a un servidor de aplicación, en donde la transmisión de la señal de autenticación al servidor de aplicación comprende transmitir la señal de autenticación por el servidor de autenticación al servidor protector de compuerta y luego transmitir la señal de autenticación por el servidor protector de compuerta al servidor de aplicación.

**SISTEMA DE AUTENTICACIÓN PARA APLICACIONES DE COMPUTADORAS
CONECTADAS EN RED**

Referencia a Solicitudes Relacionadas

Esta solicitud de patente tiene derecho de reivindicar prioridad de la Solicitud de Patente Estadounidense N° 60/531.695, presentada el 23 de diciembre de 2003, que se incorpora aquí como referencia en su totalidad.

Campo de la Invención

La presente invención se relaciona con un sistema y un método para proteger aplicaciones dentro de un sistema de computadoras conectadas en red.

Antecedentes de la Invención

Las empresas y las personas físicas dependen cada vez más de las computadoras y de la comunicación electrónica basada en computadoras. Cada vez más empresas se mudan hacia modos de operación "sin papel", y la conveniencia de la Internet ha derivado en personas físicas que utilizan medios electrónicos para diferentes actividades, tales como las comunicaciones por correo electrónico, operaciones bancarias, pago de facturas,

inversión de dinero y compras, para nombrar solamente algunas. Si bien las empresas y personas físicas desean la conveniencia de las transacciones electrónicas, estas entidades también desean mantener por lo menos el mismo nivel de seguridad que los que ofrecen los métodos transaccionales más tradicionales. Sin embargo, en muchas formas, muchas transacciones más tradicionales son implícitamente más seguros que las transacciones electrónicas porque las computadoras pueden utilizarse fácilmente para interceptar la información que se comunica entre dos o más computadoras. Por consiguiente, se han creado técnicas para asegurar la información que se está comunicando electrónicamente.

Muchas de estas técnicas utilizan diferentes aspectos de criptografía. La criptografía es el estudio de enviar y/o recibir un mensaje en una forma secreta de manera tal que solamente aquellas personas autorizadas para recibir el mensaje puedan recibirlo. Se puede utilizar la criptografía para cualquier forma de comunicación pero para los fines de esta solicitud, se discute la criptografía para la comunicación electrónica. Ejemplos de técnicas criptográficas incluyen encriptación simétrica, encriptación asimétrica y parcialización. Para la comunicación electrónica, un mensaje encriptado se puede transformar en una forma secreta que utiliza una clave de encriptación y luego se puede transformar

nuevamente en su forma original o clara con la clave de descripción.

Además de las funciones criptográficas para asegurar la información, las empresas que desean proteger la información que se almacenan electrónicamente también pueden crear relaciones de comunicación definidas entre los componentes dentro de un sistema de computadoras conectadas en red y un usuario que desea acceder a servicios dentro del sistema. Por ejemplo, un sistema de computadoras conectadas en red puede requerir que un usuario se autentique antes de poder recibir servicios desde una aplicación dentro del sistema de computadoras conectadas en red.

En un sistema de computadoras conectadas en red convencional, la autenticación del usuario puede ocurrir en cada servidor de aplicación individualmente, cada servidor de aplicación es responsable para autenticar un usuario cuando el usuario solicita los servicios de ese servidor de aplicación. Este proceso de autenticación convencional requiere que un usuario se autentique para cada servidor de aplicación que desea acceder dentro del sistema de computadoras conectadas en red.

Es deseable proporcionar un sistema y método de autenticación más eficiente, flexible y seguro para recibir servicios de un

servidor de aplicación en un sistema de computadoras conectadas en red.

Resumen de la Invención

La presente invención se relaciona con un sistema y método para autenticar un usuario dentro de un sistema de computadoras conectadas en red. El sistema comprende un usuario, un servidor de aplicación, un servidor protector de compuerta.

De acuerdo con el método de la presente invención, el usuario presenta credenciales servidor protector de compuerta, y el servidor protector de compuerta proporciona las credenciales del usuario presentadas al servidor de autenticación. El servidor de autenticación autentica al usuario. El servidor de autenticación crea una señal de autenticación al autenticar al usuario y transmite la señal de autenticación al servidor de aplicación. La transmisión de la señal de autenticación al servidor de aplicación desde el servidor de autenticación puede comprender transmitir la señal de autenticación al servidor protector de compuerta y luego al servidor de aplicación. El servidor de autenticación puede encriptar la señal de autenticación después de que se ha creado. Se prefiere que una clave de encriptación utilizada por el

servidor de autenticación para encriptar la señal de autenticación sea compartida por el servidor de autenticación y el servidor de aplicación, pero que no se comparta con el servidor protector de compuerta. El servidor de autenticación también puede firmar digitalmente la señal de autenticación después de que se ha creado. Se prefiere que el servidor de autenticación firme la señal de autenticación con un par de claves, en donde por lo menos una parte del par de claves se comparte con el servidor de autenticación y el servidor de aplicación.

Otras áreas de aplicabilidad de la presente invención se harán evidentes a partir de la descripción que se da en adelante. Se debe entender que la descripción detallada y los ejemplos específicos, si bien indican la realización preferida de la invención, tienen solamente propósitos de ilustración y no limitan el alcance de la invención.

Breve Descripción de los Dibujos

La presente invención se entenderá en forma más completa a partir de la descripción detallada y de los dibujos anexos, en donde:

La Figura 1 es una representación de un sistema de autenticación convencional para aplicaciones de computadoras conectadas en red.

La Figura 2 es una representación del sistema de computadoras conectadas en red de la presente invención.

La Figura 3 es una representación del proceso de autenticación para un usuario que comienza una sesión de identificación y que inicialmente accede a un servidor de aplicación dentro de la zona de autenticación del sistema de computadoras conectadas en red de la Figura 2.

La Figura 4 es un diagrama de flujo que representa el proceso de un servidor de identificación que autentica a un usuario.

La Figura 5 es una representación de la estructura y del contenido de la señal interior creada en la Figura 4.

La Figura 6A es un primer diagrama de flujo que ilustra el proceso de verificación que un servidor de aplicación ejecuta cuando recibe una señal interior encriptada y la identificación de la señal desde el servidor de red durante el primer tiempo.

La Figura 6B es un segundo diagrama de flujo que ilustra el proceso de verificación que ejecuta un servidor de aplicación cuando recibe una señal interior encriptada y la identificación de señal desde el servidor de red durante el primer tiempo.

La Figura 7 es un diagrama de flujo que ilustra el procesamiento de la señal interior por el servidor de red después de recibir la señal interior de regreso desde el servidor de aplicación.

La Figura 8A es una representación de la estructura y el contenido de la señal exterior creada en la Figura 7.

La Figura 8B es una representación de una señal combinada que incluye el contenido de la señal exterior y de la señal interior de las Figuras 5 y 8A.

La Figura 9 es una representación del proceso de una visita posterior por un usuario al servidor de aplicación al que accedió previamente.

La Figura 10 es un diagrama de flujo que ilustra el proceso de verificación que ejecuta un servidor de aplicación al recibir

posteriormente una señal interior encriptada y la identificación de la señal desde un servidor de red.

La Figura 11 es una representación del proceso mediante el cual un usuario accede a un segundo servidor de aplicación después de ser autenticado inicialmente por el servidor de identificación.

Descripción de las Realizaciones

La siguiente descripción de las realizaciones de la presente invención es solamente de carácter ejemplar y de ninguna manera limita la invención, su aplicación o sus usos. La presente invención tiene amplia aplicación potencial y utilidad, que se contempla que es aplicable a una amplia gama de entidades para asegurar y limitar el acceso a aplicaciones e información dentro de un sistema de computadoras conectadas en red. Por ejemplo, se contempla que el sistema y el método de autenticación para aplicaciones de computadoras conectadas en red sería beneficioso para su uso por cualquier banco presta servicios bancarios, de inversiones y/o hipotecarios en línea. Además, se contempla que el sistema y método de la presente invención sería igualmente beneficioso para la autenticación de usuarios por cualquier empresa de comercio minorista que presta servicios de comercio minorista en línea.

Además, el sistema y método de la presente invención sería beneficioso para cualquier empresa que mantiene aplicaciones e información seguras a las que acceden terceros computadoras o usuarios. La siguiente descripción se da aquí exclusivamente a modo de ejemplo con el propósito de proporcionar una revelación de la invención, pero que no limita el alcance o la sustancia de la invención.

Un sistema de computadoras conectadas en red comprende un servidor de aplicación, un sistema de base de datos, un servidor de protector de compuerta, y un usuario tal como una persona, computadora o aplicación de software. En un sistema de computadoras conectadas en red que incluye servidores de aplicación capaces de acceder a información sensible, se pueden implementar relaciones protectoras para limitar el acceso a la información sensible.

Haciendo referencia ahora a los dibujos adjuntos, la Figura 1 representa una realización de un sistema de computadoras conectadas en red convencional 10. El sistema convencional 10 puede comprender uno o más servidores de aplicación protegidos 32, 36, un sistema de base de datos protegido 28, un servidor protector de compuerta 30 y un usuario 12. Un experto en el arte entenderá que un servidor de aplicación 32, 36 puede comprender una pluralidad de funciones de aplicación (no se

muestra). En forma similar, un sistema de base de datos 28 puede comprender una pluralidad de bases de datos (no se muestran). El servidor protector de compuerta 30 conecta en forma comunicativa a los servidores de aplicación 32, 36, y el usuario 12. De hecho, el usuario 12 no puede comunicarse con los servidores de aplicación 32, 36 excepto a través del servidor protector de compuerta 30.

Para recibir servicios desde un servidor de aplicación 32 dentro del sistema 10, un usuario 12 puede poner en contacto al servidor protector de compuerta 30 y solicitar los servicios del servidor de aplicación 32 ofreciendo credenciales del usuario al servidor protector de compuerta 30 (paso 101). El servidor protector de compuerta 30 transmite las credenciales del usuario al servidor de aplicaciones 32 (paso 102), que comprende una aplicación de autenticación 33. La aplicación de autenticación 33 compara las credenciales del usuario dadas con las credenciales del usuario almacenadas en el sistema de base de datos 28 o el marco principal de la entidad operativa (no se muestra). Si el usuario 12 se autentica, el servidor de aplicación 32 crea una señal de autenticación, que comprende las credenciales del usuario. Si el usuario 12 no se autentica, la comunicación termina.

El servidor de aplicaciones 32 encripta la señal de autenticación con una clave de encriptación compartida entre todos los servidores en el sistema de computadoras conectadas en red. El servidor de aplicación 32 entonces envía la señal de autenticación encriptada y la respuesta de aplicación al servidor protector de compuerta 30 (paso 103). El servidor protector de compuerta 30 crea otra señal, es decir una señal exterior, que debe envolver la señal de autenticación. La señal exterior comprende un timbre fechador que se utiliza para asegurar que la señal exterior no se hizo antiguo. La señal exterior y la señal de autenticación juntas comprenden una señal combinada, que encripta el servidor protector de compuerta 30 con la misma clave de encriptación utilizada por el servidor de aplicación 32. El servidor protector de compuerta 30 transmite la señal combinada encriptada y una respuesta por el servidor de aplicación al usuario 12 (paso 104).

Si el usuario 12 desea acceder al servidor de aplicación 32 nuevamente, el usuario 12 presenta la señal combinada encriptada al servidor protector de compuerta 30 y solicita acceso al servidor de aplicación 32 nuevamente. El servidor protector de compuerta 30 describe la señal exterior para asegurar que la comunicación no está fuera de tiempo. Suponiendo que la señal exterior no esté fuera de tiempo, el

servidor protector de compuerta 30 presenta la señal de autenticación encriptada y el pedido del usuario 12 al servidor de aplicación 32 (paso 102). El servidor de aplicación 32 describe la señal interior y, usando la aplicación de autenticación 33, compara la información contenida en la señal interior con la información almacenada en el sistema de base de datos. Si el usuario 12 se autentica nuevamente, el servidor de aplicación 32 crea una nueva señal de autenticación, encripta la señal de autenticación y envía la señal de autenticación, junto con la respuesta del servidor de aplicación 32, al servidor protector de compuerta 30 (paso 103). El servidor protector de compuerta 30 crea una nueva señal exterior con un nuevo timbre fechador, combina la señal de autenticación y la señal exterior, encripta la señal combinada con la clave de encriptación compartida y envía la señal combinada encriptada y la señal del servidor de aplicación al usuario 12 (paso 104). Las respuestas posteriores del usuario 12 para servicios pueden seguir el procedimiento que se expuso anteriormente.

Si un usuario 12 desea acceder a un segundo servidor de aplicación 36 dentro del sistema de computadoras conectadas en red 10, el segundo servidor de aplicación 36 tiene que ejecutar el mismo proceso que el primer servidor de aplicación 32 ejecutó para autenticar al usuario 12. Este proceso

duplicador se indica con líneas punteadas de flujo que indican la comunicación entre el servidor protector de compuerta 30 y el servidor de aplicación 36 de la Figura 1. En un sistema 10, un segundo servidor de aplicación 36 no recibe el beneficio de la autenticación del usuario que ejecutada previamente por otro servidor de aplicación 32 dentro del sistema 10. Antes bien, cada servidor de aplicación posterior 36 tiene que repetir el mismo proceso para autenticar a un usuario 12 que el primer servidor de aplicación 32 ya ha ejecutado.

El sistema 10 es relativamente fácil de comprometer porque utiliza una sola clave de encriptación compartida por cada uno de los servidores del sistema 10. En este sistema 10, un usuario 12 puede limitarse a utilizar un nombre de usuario y una contraseña para la autenticación porque la funcionalidad limitada de la aplicación de autenticación 33, 35 en los servidores de aplicación 32, 36. Además, requiriendo que cada servidor de aplicación posterior dentro del sistema 10 autentique a un usuario 12 que ya ha sido autenticado por el primer servidor de aplicación consume innecesariamente tiempo para el sistema 10 y para el usuario 12. Más aún, como la señal interior del sistema 10 no tiene ninguna función fuera de tiempo, una señal interior puede teóricamente ser válida durante un período de tiempo indefinido. La disponibilidad de

las señales interiores válidas durante un período de tiempo indefinido es otra desventaja del sistema 10.

La Figura 2 representa un ejemplo del sistema de computadoras conectadas en red 110 de acuerdo con la presente invención. El sistema de computadoras conectadas en red 110 de la Figura 2 comprende los servidores de aplicación 32, 36, un sistema de base de datos 28, un servidor protector de compuerta 30, un servidor de autenticación 16 y un usuario 12. En esta realización, un servidor de identificación es el servidor de autenticación 16 y un servidor de red en el servidor protector de compuerta 30. El servidor de red 30 actúa como un eje de comunicación para el sistema de computadoras conectadas en red 110. Específicamente, el usuario 12 el servidor de identificación 16 y los servidores de aplicación 32, 36 todos se comunican con el servidor de red 30 y uno con otro a través del servidor de red 30. Además de ser el eje de comunicación para el sistema de computadoras conectadas en red 110, el servidor de red 30 también brinda una función de protector de compuerta protectora, es decir, el servidor de red 30 no transmite un pedido de usuario a un servidor de aplicación 23, 36 a menos que el usuario 12 que hace el pedido haya sido autenticado por el servidor de identificación 16. De esta manera, los servidores de aplicación 32, 36 están protegidos del usuario 12 que no ha sido autenticado. Como una forma

taquigráfica de designar la relación de comunicación entre el usuario 12, el servidor de red 30, los servidores de aplicación 32, 36 y el sistema de base de datos 28, con el cual se comunican los servidores de aplicación 32, 36, se dice que los servidores de aplicación 32, 36 y el sistema de base de datos 28 están en una zona de autenticación 20. Solamente un pedido hecho por un usuario autenticado 24 (el mejor mostrado en las Figuras 9 y 11) será transmitido por el servidor de red 30 a la zona de autenticación 20. Sin embargo, una vez que se ha autenticado al usuario 12, se le permitirá solicitar servicios de aplicación al servidor de aplicación 32, 36 dentro de la zona de autenticación 20 sin tener que ser reautenticado por el servidor de identificación 16. Un experto en el arte apreciará que una pluralidad de servidores de aplicación pueden estar ubicados dentro de la zona de autenticación y también que se puede necesitar una pluralidad de servidores de aplicación para una sola aplicación. Para los propósitos de esta solicitud, el número de referencia 12 se utiliza para designar a un usuario que no ha sido autenticado por el servidor de identificación, y el número de referencia 24 se utiliza para designar a un usuario que ha sido autenticado por el servidor de identificación 16.

El servidor de red 30 también proporciona una función protectora para el servidor de identificación 16 prohibiendo

al usuario 12 a partir de la comunicación directa con el servidor de identificación 16. El servidor de identificación 16 no recibe comunicación directa desde el usuario 12, los servidores de aplicación 32, 36 o el sistema de base de datos 28. Dado que un usuario 12 debe ser autenticado para que la comunicación del usuario 12 se pueda transmitir a la zona de autenticación 20, el servidor de identificación 16 no está ubicado en la zona de autenticación 20. Para asegurar más el servidor de identificación 16, se puede disponer una medida de seguridad adicional 26 que impide la comunicación no autorizada, tal como una barrera de fuego, entre el servidor de identificación 16 y los demás componentes del sistema 10.

La Figura 3 representa el proceso de autenticación para un usuario 12 que comienza una sesión de identificación y que inicialmente accede a un servidor de aplicación 32 dentro la zona de autenticación 20 del sistema de computadoras conectadas en red 110 de la Figura 2. Con propósitos de ejemplificación, el usuario 12 en este ejemplo puede ser una persona que intenta acceder a información de su cuenta (servidor de aplicación 32) en el sitio web de un banco (servidor de red 30). Un usuario 12 empieza presentando sus credenciales, que en este ejemplo pueden ser un nombre de usuario y contraseña, al servidor de red 30 (paso 301). Las credenciales del usuario también pueden incluir un certificado

digital, un dispositivo de hardware portátil tal como una tarjeta de identificación segura o cualquier combinación de credenciales. El protocolo de seguridad de la entidad que opera el sistema de computadoras conectadas en red 110 determina el carácter de las credenciales que se aceptarán. Además, el sistema y el método de la presente invención asume la inscripción inicial de un usuario en la entidad que opera el sistema de computadoras conectadas en red 110, mediante el cual el usuario 12 brinda información de identificación a la entidad y la entidad almacena esta información de identificación con las credenciales del usuario para la posterior autenticación. Los métodos de inscripción de este tipo son convencionales y por lo tanto aquí no se da otra explicación. El servidor de red 30 entonces presenta las credenciales del usuario al servidor de identificación 16 (paso 302).

La Figura 4 es un diagrama de flujo que representa el servidor de identificación 16 que autentica a un usuario 12. Cuando el servidor de identificación 16 recibe las credenciales del usuario del servidor de red 30 (paso 405), el servidor de identificación 16 compara las credenciales presentadas con las credenciales almacenadas para el usuario inscripto 12 (paso 415). Si los valores coinciden, se autentica al usuario 12. Sin embargo, si los valores no coinciden, entonces el servidor

de identificación 16 envía un mensaje de error de regreso al servidor de red 30 (paso 420). El servidor de red 30 entonces puede determinar si pone fin a la comunicación final o permite que el usuario 12 reingrese sus credenciales. Un experto en el arte apreciará que la comparación de las credenciales almacenadas con la credenciales presentadas es el único método de autenticar un usuario 12. Otros métodos pueden incluir la verificación algorítmica a través del intercambio de mensajes entre el servidor de identificación 16 y un usuario 12 que presenta un certificado digital o un protocolo de respuesta de desafío implementado cuando un usuario 12 utiliza una señal de hardware como sus credenciales. Sin importar cuál sea el método de autenticación utilizado, una vez que se autentica al usuario 24, el servidor de identificación 16 comienza una sesión de identificación creando una señal 50, en este ejemplo una señal interior, que identifica al usuario autenticado 24 y la sesión de identificación (paso 425).

Una ventaja de la presente invención es separar la función de identificación de la función de aplicación ya que provee flexibilidad al sistema de computadoras conectadas en red 110. En un sistema convencional, un usuario 12 se limita a ciertas credenciales debido a la funcionalidad limitada de la aplicación de autenticación 33 dentro del servidor de autenticación 32. Generalmente, es necesario que un usuario 12

tenga un nombre de usuario y una contraseña para la autenticación. En el contexto de un usuario 12 que una computadora o aplicación de software, este requerimiento es una limitación. En cambio, el sistema de la presente invención puede autenticar a cualquier usuario 12 que tiene una credencial reconocida por el servidor de red 30 y el servidor de identificación 16.

El servidor de identificación 16 de la presente invención crea una señal interior 50 con un formato definido, que es independiente de la credencial presentada por un usuario 12 para la autenticación. Los servidores de aplicación 32, 36 dentro de la zona de autenticación 20 acepta la señal interior 50 creada por el servidor de identificación 16 sin importar el tipo de credencial que un usuario 12 utilice para la autenticación. La ventaja de que el servidor de identificación autentique a un usuario 12 y cree una señal interior 50 que reconocen todos los servidores de aplicación 32, 36 dentro de la zona de autenticación 20 es que estos servidores de aplicación 32, 36 tienen la garantía de que el usuario 24 que solicita los servicios de ellos ya ha sido autenticado. Los servidores de aplicación 32, 36 dependen de la autenticación del servidor de identificación 16, específicamente la señal interior 50 creada por el servidor de identificación 16, en lugar de tener que reautenticar a un usuario 24 para cada

nuevo servidor de aplicación 32, 36 dentro de una sola sesión de identificación.

La Figura 5 representa la estructura y el contenido de la señal interior 50 creada en la Figura 4. La señal interior 50 es una estructura de datos que comprende una pluralidad de nodos de datos que almacenan información que pueden utilizarse para identificar al usuario autenticado 24 y la señal 50 en sí. La señal interior 50 comprende una identificación de señal 51, que es un identificador único para cada señal interior 50 creada. Un experto en el arte entenderá que un sistema de computadoras conectadas en red 110 puede contener servidores de identificación 16 y varios usuarios 12. Por consiguiente, el número de señales interiores 50 creadas pueden ascender a millones. Como tal, la tarea de crear una identificación de señal única 51 para todas las señales interiores 50 en un sistema de computadoras conectadas en red 110 no es insignificante. Para asegurar la exclusividad de la señal 51, se pueden utilizar valores de datos tales como la hora de la creación de señales o la identificación del servidor de identificación en la creación de la identificación de señal 51. La señal interior 50 también comprende una hora de señal 51, que representa la hora a la cual comienza la sesión de identificación y se crea o emite la señal interior 50. La hora de señal 52 es la hora oficial para la señal interior 50 y

puede utilizarse para determinar si una señal interior 50 está fuera de tiempo. El propósito y el uso de la función fuera de tiempo se explica más detalladamente a continuación.

La señal interior 50 también comprende una identificación de usuario 53, que es un identificador exclusivo para cada usuario autenticado 24. La identificación de usuario 53 puede ser un nombre de usuario o algún otro identificador insertado en la señal interior 50 por el servidor de identificación 16. Sin embargo, la identificación de usuario 53 no es necesariamente el nombre de usuario o valor de usuario ingresado por el usuario 12 cuando solicita los servicios de aplicación. La señal interior 50 también puede comprender un espacio de datos emulador 54. El espacio emulador 54 no puede llenarse con datos cada vez que se crea una señal interior 50. En cambio, el espacio de datos emulador 54 se utiliza en el caso en que un usuario autenticado 24 solicite que un tercero acceda a un servidor de aplicación 32 en la zona de autenticación 20 en representación del usuario autenticado 24. En el presente ejemplo, el espacio de datos emulador 54 puede utilizarse cuando el cliente de un banco que tiene dificultades para acceder al saldo de su cuenta solicita que un representante del servicio bancario acceda a la información de su cuenta para determinar dónde está ocurriendo el problema. En este ejemplo, se ingresa la información de la

identificación del representante del servicio en el espacio emulador 54 de la señal interior 50. Si no está ocurriendo la emulación, el espacio emulador 54 puede ajustarse a vacío.

Como se representa en la Figura 4, una vez que se ha creado la señal interior 50, el servidor de identificación firma la señal interior 50 (paso 430). La señal 50 puede firmarse digitalmente utilizando un algoritmo denominado encriptación asimétrica. La encriptación asimétrica consiste en utilizar un par de claves criptográficas para asegurar información, en este caso, una señal interior 50. Se pueden utilizar pares de claves asimétricas para encirptar un mensaje o verificar la integridad de un mensaje. Un par de claves utilizado para encriptar un mensaje está compuesta de una clave privada o una clave de descriptación, que es conocida solamente para un solo usuario o un pequeño grupo de usuarios, y una clave pública o una clave de encriptación, que pueden ser conocidas para cualquier persona. Para encriptar y descriptar un mensaje, se debe utilizar tanto la clave privada como la clave pública del par de claves. Por ejemplo, un remitente puede encriptar un mensaje utilizando la clave pública del destinatario deseado del mensaje. Una vez que el destinatario recibe el mensaje encriptado, se puede utilizar su clave privada para descriptar el mensaje. Además, como se utiliza aquí para la firma digital, se pueden utilizar pares de claves para

verificar la integridad de un mensaje. Para esta función, el par de claves comprende una clave privada o una clave de firma digital y una clave pública o una clave de verificación de firma. La clave privada puede utilizarse para firmar un mensaje o, en este caso, una señal 50. La clave pública entonces puede utilizarse para verificar la integridad de la señal 50. En esta realización, la clave de firma privada se almacena en el servidor de identificación 16, y se puede utilizar un servidor de aplicación 32, 36 para la clave de verificación pública del servidor de identificación para verificar la integridad de la señal interior firmada 50 verificando la firma 55. Se puede utilizar cualquier función de encriptación asimétrica y función de firma digital asimétrica. Las funciones de encriptación asimétricas incluyen, en forma no taxativa, RSA, ElGamal y variantes de ellas, y ElGamal de Curva Elíptica y variantes de él. Las funciones de firma digital asimétrica incluyen, en forma no taxativa, RSA, DSA o DSS (Algoritmo/Estándar de Firma Digital de Estados Unidos) y ECDSA (DSA de Curva Elíptica).

Después de que la señal interior 50 se ha firmado digitalmente, el servidor de identificación 16 encripta la señal interior 50 (paso 435). Si bien la señal interior 50 no tiene ninguna limitación de tamaño, es preferible que la señal 50 sea lo más compacta que sea posible. Es más preferible que

la señal interior 50 sea menor o igual a dos kilobytes. Un experto en el arte, sin embargo, reconocerá que el nivel de compactación depende del método de encriptación empleado. En la presente realización, el servidor de identificación 16 encripta la señal interior firmada 50 con una clave de encriptación simétrica. Un mensaje se bloquea (encripta) con una clave y luego la misma clave se utiliza para desbloquear (descriptar) el mensaje. Para proteger un mensaje cuando utiliza la encriptación simétrica, es vital tener un método seguro para intercambiar la clave secreta a todos los usuarios. Se puede utilizar cualquier función de encriptación simétrica. Las funciones de encriptación simétrica incluyen, en forma no taxativa, AES, DES, 3DES, IDEA, RC5, RC6.

En la presente invención, la clave simétrica utilizada para encriptar la señal interior firmada 50 se comparte con los servidores de identificación 16 del sistema de computadoras conectadas en red 110 y los servidores de aplicación 32, 36 dentro de la zona de autenticación 20. La clave simétrica no se comparte con el servidor de red e30. Este aspecto del sistema de la presente invención es una ventaja sobre los sistemas convencionales 10 porque el servidor de red 30 no puede acceder a la señal interior encriptada 50 creada por el servidor de identificación 16. El acceso limitado a la señal interior 50 proporciona más seguridad para la información

contenida en ella. Si se utiliza la encriptación asimétrica, se utiliza un par de claves asimétricas diferentes de una utilizada para firmar la señal interior 50 para la encriptación y descriptación de la señal interior 50. En esta realización, el servidor de identificación 16 encriptaría la señal interior 50 con la clave pública del par de claves del servidor de aplicación particular 32, 36 al cual el usuario autenticado 24 desea acceder. El servidor de aplicación respectivo 32, 36 podría descriptar la señal interior 50 con su clave privada que coincide con la clave pública utilizada para encriptar la señal interior 50. Si se utiliza la encriptación asimétrica en la presente realización, se prefiere que todos los servidores de aplicación 32, 36 dentro de la zona de autenticación 20 utilicen el mismo par de claves de encriptación asimétrica. De esta manera, el servidor de identificación 16 podría utilizar la misma clave pública para encriptar las señales interiores 50 para todos los servidores de aplicación 32, 36 dentro de la zona de autenticación.

Después de que se encripta la señal interior firmada 50 (paso 435), el servidor de identificación 16 envía la señal interior encriptada 50 al servidor de red 30 junto con la identificación de señal 51 (paso 440 y 303). El servidor de red 30 envía una copia de la señal interior encriptada 50 y la identificación de señal 51 a un servidor de aplicación

particular 32 en la zona de autenticación 20 (paso 304). Sin embargo, la comunicación del servidor de red 30 al servidor de aplicación 32 es una comunicación sincrónica en que el servidor de red 30 conserva una copia de la señal interior encriptada 50 y la identificación de señal 51 y envía una copia de cada una al servidor de aplicación 32. El servidor de red 30 espera una respuesta del servidor de aplicación 32 antes de continuar cualquier acción. Las Figuras 6A y 6B representan el proceso de verificación que el servidor de aplicación 32 ejecuta una vez que recibe la señal interior encriptada 50 y la identificación de señal 51 (paso 605). El servidor de aplicación 32 describe la señal interior encriptada 50 utilizando la clave simétrica compartida (paso 610). Sin embargo, la descripción de la señal interior 50 no es un proceso destructivo, es decir después de que la señal interior 50 se describe, el servidor de aplicación 32 posee tanto la señal interior encriptada 50 como sus contenidos descritos. El servidor de aplicación 32 compara la identificación de señal 51 de la señal interior 50 con la identificación de señal presentada por el servidor de identificación 16 (paso 615). Si los valores de identificación de señal coinciden, el servidor de aplicación 32 continúa el proceso de verificación. Si los valores de identificación de señal no coinciden, el servidor de aplicación 32 envía un mensaje de error al servidor de red 30 (paso 620). El servidor

de red 30 luego determina si pone fin a la sesión de identificación o permite que el usuario 24 reingrese sus credenciales.

Suponiendo que los valores de identificación de señal coincidan, el servidor de aplicación 32 verifica la hora de la señal 52 para verificar que la sesión de identificación no está fuera de tiempo (paso 625). Específicamente, el servidor de aplicación 32 resta la hora de la señal 52 a la hora real para determinar si ha existido la duración que la señal interior 50. El servidor de aplicación 32 luego compara el tiempo de existencia con su función fuera de tiempo. Si la señal interior 50 ha existido durante menos tiempo que el provisto en la función fuera de tiempo, entonces la sesión de identificación continúa. Cada servidor de aplicación 32, 36 dentro de un sistema de computadoras conectadas en red 110 tiene un protocolo de seguridad, que incluye una función fuera de tiempo. La función fuera de tiempo determina el tiempo durante el cual un usuario autenticado 24 puede utilizar una señal interior 50. La funcionalidad del servidor de aplicación 32, 36 determina el tiempo durante el cual la función fuera de tiempo para el servidor de aplicación 32, 36. Para la presente realización, un ejemplo de función fuera de tiempo puede ser de 30-90 minutos.

Si una señal interior 50 no está fuera de tiempo, el servidor de aplicación verifica la firma de la señal interior que utiliza la clave pública del servidor de identificación 16 (paso 630). Finalmente, el servidor de aplicación 32 verifica que el usuario autenticado 24 es un suscriptor del servidor de aplicación particular 32 al que se está accediendo (paso 635). En el presente ejemplo, esto incluiría el servidor de operaciones bancarias que verifica que el usuario autenticado 24 es un suscriptor del servicio de operaciones bancarias en línea del banco. Si alguno de los pasos 625, 630, 635 tiene un resultado negativo, el servidor de aplicación 32 envía un mensaje de error al servidor de red 30 (paso 640). Una vez que todos los pasos de verificación se completan con éxito, el servidor de aplicación 32 comienza una sesión de aplicación para el usuario autenticado 24 (paso 1645). Según el servidor de aplicación particular 32 al que se está accediendo, el servidor de aplicación 32 puede crear una señal de aplicación cuando empieza la señal de aplicación para enviar al usuario autenticado 24. Algunos servidores de aplicación 32, 36 crean señales de aplicación para enviar a los usuarios 24 y algunos no lo hacen. Si un servidor de aplicación 32, 36 crea una señal de aplicación no afecta la funcionalidad del sistema de autenticación y el método de la presente invención.

Después de que ha comenzado una sesión de aplicación, el servidor de aplicación 32 calcula un valor parcializado para la señal interior encriptada 50 y almacena el valor parcializado en su propio almacenamiento o en el sistema de base de datos 28 de la zona de autenticación 120 (paso 635). La parcialización consiste en transformar un mensaje de entrada de cualquier tamaño en un valor de salida o parcializado de otro tamaño generalmente más pequeño utilizando un algoritmo matemático. El valor parcializado se denomina digesto de mensaje. El digesto de mensaje es una "huella digital" del mensaje de entrada y sirve para mantener la integridad del mensaje parcializado permitiendo que un destinatario verifique que el mensaje no se alteró desde que se parcializó. El valor parcializado luego se almacena en la zona de autenticación 20 por la duración de la sesión de aplicación particular.

El servidor de aplicación 32 envía una respuesta del servidor de aplicación y una señal de aplicación (si se crea) al servidor de red 30 (paso 305 y 660). La Figura 7 representa el servidor de red 30 que crea una señal exterior 70 (paso 710) y envolviendo la señal interior 50 para formar una señal combinada 60 (paso 715).

La Figura 8A representa la señal exterior 71 y su contenido. La señal exterior 71 es una estructura de datos que comprende una pluralidad de nodos de datos que almacenan información que pueden usarse para asegurar la integridad de la señal en sí. La señal exterior 70 comprende la misma identificación de señal 51 que está en la señal interior 50. También puede incluir un período de tiempo de arrollamiento 64 (RTP). El período de tiempo de arrollamiento 64 es el tiempo durante el cual la señal exterior 70 es válida. En el presente ejemplo, se entiende que el período de tiempo de arrollamiento cubre el tiempo entre cada clic del mouse de la computadora del usuario autenticado 24. La señal exterior 70 también puede incluir un timbre de hora de arrollamiento 65 (RTS). El timbre de hora de arrollamiento 65 es la hora a la cual se crea la señal exterior 70. En el presente ejemplo, el timbre de hora de arrollamiento 65 se indica en segundo. Para determinar si la señal exterior 70 está fuera de tiempo, el servidor de red 30 resta el timbre de hora de arrollamiento 65 a la hora real y compara el valor del período de tiempo de arrollamiento 64. Siempre que la diferencia sea menor que el período de tiempo de arrollamiento 64, la señal exterior 70 no está fuera de tiempo, es decir la señal exterior es válida. La señal exterior 70 también puede incluir un soporte de lugar 68 para indicar si la señal 70 es una señal de uso normal o una señal de emulación.

La señal exterior 70 puede incluir un indicador de estado de autenticación (AST) 69, que indica la forma de autenticación que utilizó el servidor de identificación 16. La autenticación requerida para un servidor de aplicación 32 puede variar según los requisitos de seguridad para el servidor de aplicación 32. Como tales, algunos servidores de aplicación 32 pueden requerir una forma de autenticación específica. La señal exterior 70 también puede incluir un soporte de lugar 75 para los datos específicos de la aplicación. Por ejemplo, algunos servidores de aplicación 32 requieren datos que otros servidores de aplicación 36 no requieren y que no están incluidos en ninguna otra parte de la señal exterior 70 o la señal interior 50. El campo específico de la aplicación 75 de la señal exterior 70 puede alojar cualquier información adicional que requiere un servidor de aplicación 32. Un experto del arte reconocerá que se pueden agregar campos adicionales a la señal exterior 70 necesaria para cualquier servidor de aplicación particular 32 o sistema de computadoras conectadas en red 110. El indicador de estado de autenticación 69 y el campo específico de la aplicación 75 son opcionales. Cuando la señal interior 50 y la señal exterior 70 se combinan, la señal combinada 60 incluye un rótulo de clave de señal interior 66. El rótulo de clave de señal interior 66 indica la clave de encriptación utilizada para encriptar la señal interior 50. Un rótulo de clave 66 es útil en un sistema

de computadoras conectadas en red 110 en el cual las claves de encriptación se renuevan y rotan.

Como se indica en la Figura 7, una vez que la señal exterior 70 se crea y se envuelve con ella a la señal interior 50, la señal combinada 60 se parcializa utilizando una clave de código de autenticación basada en la parcialización (clave HMAC) (paso 720). Se puede utilizar cualquier función para la clave HMAC que incluye, en forma no taxativa, MD5, SHA-1, SHA-232, SHA-256, SHA-504 y SHA-512. Un valor parcializado o código de autenticación de mensaje (MAC) 71 que contiene el resultado de la función parcializada sincronizada está unido a la señal combinada 60. El servidor de red 30 encripta la señal combinada 60 con una clave simétrica que se comparte entre cada servidor de red 30 del sistema de computadoras conectadas en red 110 (paso 725). La clave simétrica utilizada para encriptar la señal combinada 60 no se comparte con el servidor de aplicación 32, 36 y el servidor de identificación 16. Si bien la señal combinada 60 no tiene ninguna limitación de tamaño, es preferible que la señal 60 sea lo más compacta que sea posible. Es más preferible que la señal combinada 60 sea menor o igual a 2 kilobytes. Un experto en el arte, sin embargo, reconocerá que el nivel de compactación depende del método de encriptación empleado.

Un rótulo de clave de señal exterior 61 que indica las claves utilizadas para encriptar y parcializar la señal combinada 60 está unido a la señal combinada encriptada 60. Un sistema de computadoras conectadas en red 110 en donde todas las claves no son conocidas para todos los servidores es una ventaja sobre el sistema convencional 10. En el sistema de la presente invención, por lo menos el servidor de identificación 16, el servidor de red 30 y el servidor de aplicación 32 cooperan para proporcionar los servicios de aplicación solicitados. El sistema entre los servidores brinda mayor seguridad para los servidores de aplicación 32, 26 e información dentro de la zona de autenticación 20.

Una vez que la señal combinada 60 se encripta, el servidor de red 30 envía la respuesta de aplicación, que incluye la señal combinada encriptada 60 y la señal de aplicación (si se crea) al usuario autenticado 24 (paso 306). En este ejemplo, éste es el punto en que el usuario autenticado 24 en el sitio web del banco tiene acceso a su cuenta bancaria. Se puede observar información tal como el saldo de una cuenta de cheques, el saldo de una caja de ahorro, etc.

Generalmente, sin embargo, un usuario autenticado 24 desea hacer más que sólo acceder inicialmente a un servidor de aplicación 32. Un usuario autenticado 24 puede desear visitar

el servidor de aplicación 32 muchas veces en una sesión de aplicación para solicitar información o servicios adicionales. Por ejemplo, el usuario autenticado 24 que accede a su cuenta bancaria, puede desear ver las transacciones con cheques o tarjeta débito, que se han procesado desde su último estado de cuenta o transferencia de dinero desde su cuenta de cheques a su caja de ahorro. Cualquiera de estos pedidos de información o servicios constituye visitas adicionales al servidor de aplicación al que se accedió inicialmente.

La Figura 9 representa el proceso para que un usuario autenticado 24 visite posteriormente un servidor de aplicación al que accedió previamente. El usuario autenticado 24 solicita una visita posterior al servidor de aplicación 32 presentando la señal combinada 60 y la señal de aplicación (si se crea) al servidor de red 30 (paso 901). En el presente ejemplo, el usuario autenticado puede desear ver el número de transacciones con tarjetas de débito que se han procesado desde el último estado de cuenta. Para hacerlo, hará clic en la parte del sitio web que solicita acceso a las transacciones con tarjeta de débito. Cuando hace esto, la señal combinada 60 y señal de operación bancaria en línea se devuelve al servidor de red 30.

El servidor de red 30 describe la señal combinada 60 que utiliza la clave simétrica de servidor de red. Un experto en el arte entenderá que el sistema de computadoras conectadas en red puede incluir servidores de red 30. Por consiguiente, el mismo servidor de red 30 que creó inicialmente la señal exterior 70 y encriptó la señal combinada 60 puede no ser el servidor de red 30 que recibe el pedido del usuario autenticado 24 en una vista posterior. La utilización de una clave de encriptación simétrica que se comparte entre los servidores de red 30 del sistema de computadoras conectadas en red 110 permite que cualquier servidor de red 30 del sistema describe la señal combinada 60 encriptada por cualquier servidor de red 30 del sistema. Después de que la señal combinada 60 se describe, el servidor de red 30 calcula un valor parcializado para la señal combinada 60 utilizando la clave HMAC indicada por el rótulo de clave exterior 61 y compara este valor parcializado calculado con el valor parcializado 71 almacenado con la señal combinada 60. Suponiendo que los valores parcializados coincidan, el servidor de red 30 verifica que la señal exterior 71 no está fuera de tiempo, es decir que no se ha excedido el período de tiempo de arrollamiento 64.

La Figura 10 representa el proceso de verificación de que ejecuta un servidor de aplicación 32 en la vista posterior

por el usuario autenticado 24. El servidor de red 30 envía la señal interior encriptada 50, la identificación de señal 51 y la señal de aplicación (si se crea) al servidor de aplicación 32 (paso 904 y 1005). En visitas posteriores al servidor de aplicación 32, el servidor de aplicación 32 no tiene que ejecutar la misma verificación que se ejecutó en la visita inicial del usuario autenticado 24. En cambio, el servidor de aplicación 32 puede calcular una parcialización de la señal interior encriptada 50 (paso 1010) y comparar el valor parcializado con el valor parcializado que se computó y se almacenó durante la verificación del usuario (paso 1015). La verificación de un usuario autenticado 24 con una función parcializada en visitas posteriores es más rápida que la verificación del usuario en una visita inicial y guarda la funcionalidad de computadora sin sacrificar la seguridad. El servidor de aplicación 32 también verifica su señal de aplicación (si se crea) en visitas posteriores de un usuario autenticado 24 y verifica que la señal 50 no está fuera de tiempo (paso 1025). Si el paso 1015 o 1025 tienen un resultado negativo, el servidor de aplicación 32 envía un mensaje de error al servidor de red 30 (paso 1020). Una vez que la verificación es completa, el servidor de aplicación 32 procesa el pedido, actualiza su señal de aplicación (si se crea) (paso 1030), y envía una respuesta de aplicación al servidor de red 30 (paso 905 y 1040).

El servidor de red 30 actualiza el timbre de tiempo de arrollamiento 165 en la señal exterior 70, calcula un nuevo valor parcializado 171 para la señal combinada 60 y encripta la señal combinada 60. El servidor de red 30 devuelve la respuesta de aplicación que incluye la señal combinada encriptada 60 y la señal de aplicación (si se crea) al usuario autenticado 24 (paso 906). En el presente ejemplo, el usuario autenticado 24 puede ver todas las transacciones de débito ya desde su último estado de cuenta. El proceso de la Figura 9 ocurre para cada pedido de usuario posterior de acceso a un servidor de aplicación 32, es decir una vez que el servidor de aplicación 32 ha verificado un usuario autenticado 24 dentro de una sola sesión de identificación, se seguirá el proceso de la Figura 9 para cada pedido posterior a ese servidor de aplicación 32 por el usuario autenticado 24.

Un usuario autenticado 24 puede desear acceder a otro servidor de aplicación 36 dentro de la zona de autenticación 20 durante una sesión de identificación. Por ejemplo, el usuario autenticado 24 puede desear acceder a sus cuentas de corretaje mientras se identifica en el sitio web del banco. La Figura 11 representa el proceso de un usuario autenticado 24 que accede a un segundo servidor de aplicación 36 después de ser inicialmente autenticado por el servidor de identificación 16. Cuando un usuario autenticado solicita acceso a un segundo

servidor de aplicación 36 en una sola sesión de identificación, el usuario autenticado 24 tiene una señal combinada encriptada 60 y una señal de aplicación desde el primer servidor de aplicación 32 (si se crea).

El usuario autenticado 24 presenta la señal combinada encriptada 60 y la señal de aplicación desde el primer servidor de aplicación 32 al servidor de red 30 y solicita acceso a un segundo servidor de aplicación 36 (paso 1101). El servidor de red 30 describe la señal combinada 60, verifica la integridad de la señal combinada 60 comparando un valor parcializado calculado al valor parcializado 71 almacenado con la señal combinada 60, y verifica que la señal exterior 70 no está fuera de tiempo. El servidor de red 30 presenta la señal interior encriptada 50 y la identificación de señal 51 al segundo servidor de aplicación 36 (paso 1104). Dado que ésta es la primera vez que el segundo servidor de aplicación 36 se ha presentado con un pedido para el usuario autenticado 24, el segundo servidor de aplicación 36 verifica el usuario autenticado 24 en la misma forma en que lo hizo el primer servidor de aplicación 32 en la visita inicial. Específicamente, el servidor de aplicación 32 describe la señal interior encriptada 50 que utiliza la clave simétrica compartida. El servidor de aplicación 36 verifica que la identificación de señal 50 de la señal interior 50 coincide

con la identificación de señal 51 provista por el servidor de red 30. El segundo servidor de aplicación 36 luego verifica que la hora de señal 52 para verificar que la sesión de identificación no está fuera de tiempo. El segundo servidor de aplicación 36 verifica la firma de la señal interior 50 utilizando la clave pública del servidor de identificación 16. Finalmente, el segundo servidor de aplicación 36 verifica que el usuario autenticado 24 es un suscriptor del servidor de aplicación particular 36 al cual se accedió. En el presente ejemplo, el servidor de corretaje verifica que el usuario autenticado 24 es un suscriptor del servicio de corretaje en línea del banco. Una vez que todos los pasos se completan exitosamente, el segundo servidor de aplicación 36 comienza una sesión de aplicación para el usuario autenticado 24. Según el servidor de aplicación 36 al que se acceda, el servidor de aplicación 36 puede crear una señal de aplicación para enviar al usuario autenticado 24.

Después de que ha comenzado una sesión de aplicación, el servidor de aplicación 36 calcula un valor parcializado para la señal interior encriptada 50 y almacena el valor parcializado en su propio almacenamiento o en el sistema de base de datos 28 de la zona de autenticación 20. El valor parcializado se almacena en la zona de autenticación 20 durante la sesión de aplicación particular.

El segundo servidor de aplicación 36 envía una respuesta de aplicación que incluye la señal de aplicación (si se crea) al servidor de red 310 (paso 1105). El servidor de red 30 crea una señal exterior 70 que envuelve la señal interior encriptada 50 para formar una señal combinada 60. Una vez que la señal exterior 70 se crea y envuelve la señal interior 50, un valor parcializado se calcula para la señal combinada 60. Un valor parcializado 71 que contiene el resultado de la función parcializada sincronizada se une a la señal combinada 60. El servidor de red 30 encripta la señal combinada 60 con una clave simétrica que es conocida para todos los servidores de red 30, y un rótulo de clave de señal exterior 61 que indica las claves utilizadas para encriptar y parcializar la señal combinada 60 se une a la señal combinada encriptada 60. Una vez que la señal combinada 60 se encripta y parcializa, el servidor de red 30 envía la señal combinada encriptada 60 y la señal de aplicación (si se crea) con la respuesta de aplicación al usuario autenticado 24 (paso 1106). En este ejemplo, el usuario autenticado 24 en el sitio web del banco tiene acceso a su cuenta de corretaje. El proceso representado en la Figura 11 puede utilizarse para acceder a cualquier servidor de aplicación posterior dentro de una sola sesión de identificación.

Los procesos descritos anteriores, a saber acceder a un primer servidor de aplicación en la identificación inicial, posteriormente acceder a un servidor de aplicación después de la identificación y acceder a un segundo servidor de aplicación después de la identificación, abarcan el alcance de las interacciones que puede desear un usuario cuando accede a servidores de aplicación dentro de una zona de autenticación. Si bien anteriormente se dieron ejemplos para un usuario que es una persona que accede a servidores de aplicación a través de un servidor de red, el sistema y el método de la presente invención es igualmente aplicable a un usuario tal como una aplicación de computadora o una función de software que accede a un servidor de aplicación dentro de una zona protegida.

El sistema de autenticación para las aplicaciones de computadoras protegidas proporcionan varias ventajas sobre los sistemas de autenticación conocidos. El sistema de la presente invención es más seguro que los sistemas convencionales. En el presente sistema, el conocimiento de las claves de encriptación se separa por funcionalidad de servidor, mientras que, en los sistemas convencionales todos los servidores conocen todas las claves de encriptación. La separación de claves por funcionalidad asegura que por lo menos tres servidores dentro del sistema de autenticación debe cooperar para completar un pedido de usuario. De esta manera, un mal

actor no puede comprometer el sistema de autenticación completo comprometiendo solamente a un servidor. En cambio, la comunicación termina y se prohíbe al mal actor ingresar a la zona de protección. Por consiguiente, el sistema de la presente invención garantiza una mayor seguridad dentro del sistema de autenticación.

Además, la separación de la funcionalidad de identificación de la funcionalidad de aplicación proporciona mayor flexibilidad y seguridad dentro del sistema de autenticación. Las aplicaciones y la información dentro de la zona de autenticación son accesibles para más tipos de usuarios ya que un usuario no se ve limitado a solamente utilizar un nombre de usuario y contraseña como una credencial para la autenticación. Además, los aspectos de la señal interior proporcionan mayor seguridad para el sistema de la presente invención. La firma digital en señal interior verifica que una entidad diferente del servidor de identificación no ha comprometido y no ha creado la señal interior. La función fuera de tiempo de la señal interior asegura que una señal interior no es válida durante un período de tiempo indefinido. La identificación de señal única creada por el servidor de identificación proporciona mayor protección al sistema de autenticación. Colocando la identificación de señal única en la señal exterior e interior, el sistema es menos vulnerable a los ataques de "cortar y pegar" mediante los cuales un mal

actor intenta ingresar en la zona protegida combinando una señal exterior y una señal interior que no se crearon para ser combinadas, por ejemplo combina una señal interior con el tiempo restante con una señal exterior nueva cuando la señal exterior creada para la señal interior está fuera de tiempo. Dado que la identificación de señal única se coloca tanto en la señal exterior como en la señal interior, será rápidamente evidente en el ataque de tipo de cortar y pegar que las identificaciones de señales no coinciden.

En consecuencia los expertos en el arte entenderán rápidamente que la presente invención es susceptible de amplia utilidad y aplicación. Muchas realizaciones y adaptaciones de la presente invención diferentes de aquellas descritas aquí, así como muchas variaciones, modificaciones y disposiciones equivalentes, serán evidentes o sugeridas por la presente invención y la descripción precedente de ella, sin apartarse de la esencia o del alcance de la presente invención. Por consiguiente, si bien se debe entender que esta descripción es sólo ilustrativa y ejemplar de la presente invención y se hace solamente con los propósitos de brindar una descripción completa de la invención. La descripción precedente no desea o no se debe interpretar que limita la presente invención o excluye de otro modo todas aquellas otras realizaciones, adaptaciones, variaciones modificaciones y disposiciones equivalentes.

REIVINDICACIONES

1. Un método de autenticar a un usuario con un servidor de autenticación en un sistema de computadoras conectadas en red, el método comprende:

- (a) presentar credenciales de usuario por un usuario a un servidor protector de compuerta;
- (b) proporcionar las credenciales de usuario por un servidor protector de compuerta a un servidor de autenticación;
- (c) autenticar al usuario por el servidor de autenticación;
- (d) crear una señal de autenticación por el servidor de autenticación al ocurrir la autenticación del usuario; y
- (e) transmitir la señal de autenticación por el servidor de autenticación a un servidor de aplicación, en donde la transmisión de la señal de autenticación al servidor de aplicación comprende transmitir la señal de autenticación por el servidor de autenticación al servidor protector de compuerta y luego transmitir la señal de autenticación por el servidor protector de compuerta al servidor de aplicación.

2. El método de autenticar un usuario de acuerdo con la reivindicación 1, que además comprende prestar servicios de aplicación por un servidor de aplicación al usuario.

3. El método de autenticar un usuario de acuerdo con la reivindicación 1, que además comprende firmar digitalmente la señal de autenticación por el servidor de autenticación.

4. El método de autenticar un usuario de acuerdo con la reivindicación 3, que además comprende utilizar la firma digital para verificar la señal de autenticación.

5. El método de autenticar un usuario de acuerdo con la reivindicación 4, en donde el servidor de aplicación verifica la señal de autenticación.

6. El método de acuerdo con la reivindicación 1, que además comprende verificar la señal de autenticación por el servidor de aplicación.

7. El método de autenticar un usuario de acuerdo con la reivindicación 1, en donde la señal de autenticación comprende una pluralidad de nodos de datos almacenados en ella que representan una estructura de datos.

8. El método de autenticar un usuario de acuerdo con la reivindicación 7, en donde la estructura de datos comprende:

(a) un primer nodo de datos que comprende datos que incluyen la hora a la que se creó la estructura de datos;

(b) un segundo nodo de datos que comprende datos que representan el usuario; y

(c) un tercer nodo de datos que comprende datos únicos que identifican la estructura de datos.

9. El método de autenticar un usuario de acuerdo con la reivindicación 1, que además comprende encriptar la señal de autenticación por el servidor de autenticación.

10. El método de autenticar un usuario de acuerdo con la reivindicación 9, en donde la encriptación de la señal de autenticación comprende utilizar una clave de encriptación compartida por el servidor de autenticación y el servidor de aplicación para encriptar la señal de autenticación.

11. El método de autenticar un usuario de acuerdo con la reivindicación 10, que además comprende descriptar la señal de autenticación por el servidor de aplicación.

12. El método de autenticar un usuario de acuerdo con la reivindicación 11, además comprende transmitir la señal de autenticación por el servidor de aplicación al servidor protector de compuerta después de transmitir la señal de autenticación por el servidor de autenticación al servidor de aplicación.

13. El método de autenticar un usuario de acuerdo con la reivindicación 12, que además comprende crear una señal de usuario por el servidor protector de compuerta.

14. El método de autenticar un usuario de acuerdo con la reivindicación 13, que además comprende envolver la señal de autenticación con la señal exterior.

15. El método de autenticar un usuario de acuerdo con la reivindicación 1, en donde el usuario es una persona física.

16. El método de autenticar un usuario de acuerdo con la reivindicación 1, en donde el usuario es una computadora.

17. El método de autenticar un usuario de acuerdo con la reivindicación 1, en donde el usuario es una función de software.

18. El método de autenticar un usuario de acuerdo con la reivindicación 1, en donde las credenciales del usuario comprenden un nombre de usuario y contraseña.

19. El método de autenticar un usuario de acuerdo con la reivindicación 1, en donde la autenticación del usuario por el servidor de autenticación comprende comparar las credenciales

de usuario presentadas con credenciales de usuario almacenadas.

20. El método de autenticar un usuario de acuerdo con la reivindicación 1, en donde las credenciales del usuario comprenden un certificado digital.

21. El método de autenticar un usuario de acuerdo con la reivindicación 20, en donde la autenticación del usuario por el servidor de autenticación comprende verificar la identidad del usuario intercambiando mensajes entre el servidor de autenticación y el usuario.

22. El método de autenticar un usuario de acuerdo con la reivindicación 1, en donde las credenciales de usuario comprenden un dispositivo portátil que contiene datos que identifican al usuario.

23. El método de autenticar un usuario de acuerdo con la reivindicación 1, en donde las credenciales del usuario comprenden una entrada de usuario y un valor generado por un dispositivo portátil que verifica la entrada de usuario.

24. Un sistema de autenticación dentro de un sistema de computadoras conectadas en red, que comprende:

un usuario;

un servidor de aplicación;

un servidor de autenticación separado del servidor de aplicación utilizado para autenticar un usuario; y

una señal de autenticación generada por el servidor de autenticación, en donde la señal de autenticación es utilizada por el servidor para verificar que el usuario ha sido autenticado por el servidor de autenticación.

25. El sistema de autenticación de acuerdo con la reivindicación 24, en donde el servidor de autenticación está conectado en forma comunicativa con el sistema de computadoras conectadas en red.

26. El sistema de autenticación de acuerdo con la reivindicación 24, en donde la comunicación con el servidor de autenticación está controlada por un dispositivo protector.

27. El sistema de autenticación de acuerdo con la reivindicación 26, en donde el dispositivo protector es una barrera de fuego.

28. El sistema de autenticación de acuerdo con la reivindicación 24, que además comprende un servidor protector

de compuerta conectado en forma comunicativa con el servidor de aplicación y el servidor de autenticación.

29. El sistema de autenticación de acuerdo con la reivindicación 28, en donde el servidor de autenticación recibe la comunicación directa solamente desde el servidor protector de compuerta.

30. El sistema de autenticación de acuerdo con la reivindicación 28, en donde el servidor de aplicación recibe la comunicación directa solamente desde el servidor protector de compuerta.

31. Un método de autenticar un usuario dentro de un sistema de computadoras conectadas en red, el método comprende:

- (a) proporcionar un servidor de autenticación para autenticar un usuario;
- (b) crear una señal de autenticación por el servidor de autenticación cuando ocurre la autenticación del usuario;
- (c) proporcionar un servidor de aplicación;
- (d) proporcionar una primera clave de encriptación, dicha primera clave de encriptación es compartida por el servidor de autenticación y el servidor de aplicación; y
- (e) encriptar la señal de autenticación con la primera clave de encriptación.

32. El método de autenticar un usuario de acuerdo con la reivindicación 31, que además comprende:

(a) proporcionar una segunda clave de encriptación, dicha segunda clave de encriptación es un par de claves asimétricas en donde el servidor de autenticación almacena la clave privada del par de claves asimétricas; y

(b) firmar digitalmente la señal de autenticación por el servidor de autenticación con la clave privada del par de claves asimétricas antes de encriptar la señal de autenticación con la primera clave de encriptación.

33. El método de autenticar un usuario de acuerdo con la reivindicación 32, que además comprende proporcionar un servidor protector de compuerta.

34. El método de autenticar un usuario de acuerdo con la reivindicación 33, que además comprende proporcionar una tercera clave de encriptación, la tercera clave de encriptación se almacena en el servidor protector de compuerta.

35. El método de autenticar un usuario de acuerdo con la reivindicación 34, en donde la tercera clave de encriptación es una clave simétrica.

36. El método de autenticar un usuario de acuerdo con la reivindicación 34, que además comprende proporcionar una pluralidad de servidores de autenticación, servidores de aplicación y servidores protectores de compuerta, en donde la clave de encriptación se comparte entre los servidores de autenticación y los servidores de aplicación, la clave privada de la segunda clave de encriptación se almacena en los servidores de autenticación y la tercera clave de encriptación se comparte entre los servidores protectores de compuerta.

37. Un sistema de autenticación dentro de un sistema de computadoras conectadas en red, que comprende:

- (a) un servidor de aplicación;
- (b) un servidor protector de compuerta;
- (c) un servidor de autenticación; y
- (d) una primera clave de encriptación compartida por el servidor de aplicación y el servidor de autenticación, en donde la primera clave de encriptación no se comparte con el servidor protector de compuerta.

38. El sistema de autenticación de acuerdo con la reivindicación 37, que además comprende una segunda clave de encriptación, la segunda clave de encriptación es un par de claves asimétricas, en donde el servidor de autenticación almacena la clave privada del par de claves asimétricas y el

servidor de aplicación almacena la clave pública del par de claves asimétricas.

39. El sistema de autenticación de acuerdo con la reivindicación 37, en donde la primera clave de encriptación es una clave simétrica.

40. El sistema de autenticación de acuerdo con la reivindicación 37, que además comprende una tercera clave de encriptación almacenada por el servidor protector de compuerta, en donde la tercera clave de encriptación no es almacenada por el servidor de aplicación o el servidor de autenticación.

41. El sistema de autenticación de acuerdo con la reivindicación 39, en donde la tercera clave de encriptación es una clave simétrica.

42. Una señal legible por una computadora que tiene una pluralidad de nodos de datos almacenados en ella y que representa una estructura de datos para verificar la autenticación de un usuario, que comprende:

(a) un primer nodo de datos que comprende datos que identifican la estructura de datos;

(b) un segundo nodo de datos que comprende datos que indican la hora a la cual se creó la estructura de datos; y

(c) un tercer nodo de datos que comprende datos únicos que representan al usuario.

43. La señal legible por una computadora de acuerdo con la reivindicación 42, que además comprende un cuarto nodo de datos que comprende datos que representan la relación entre el usuario y el solicitante.

44. La señal legible por una computadora de acuerdo con la reivindicación 42, en donde el tercer nodo de datos se obtiene de las credenciales presentadas por el usuario.

45. La señal legible por una computadora de acuerdo con la reivindicación 42, en donde el primer nodo de datos comprende datos obtenidos del segundo nodo de datos.

46. La señal legible por una computadora de acuerdo con la reivindicación 42, en donde el primer nodo de datos comprende datos obtenidos de datos que identifican a un servidor.

47. La señal legible por una computadora de acuerdo con la reivindicación 42, que además comprende una segunda estructura

de datos para asegurar datos almacenados dentro de la primera estructura de datos.

48. La señal legible por una computadora de acuerdo con la reivindicación 47, en donde la segunda estructura de datos comprende:

- (a) un quinto nodo de datos que comprende los datos del primer nodo de datos;
- (b) un sexto nodo de datos que comprende datos que indican la hora a la cual se creó la segunda estructura de datos; y
- (c) un séptimo nodo de datos que comprende datos que indican el período de tiempo durante el cual la segunda estructura de datos es válida.

49. La señal legible por una computadora de acuerdo con la reivindicación 48, en donde un servidor ejecuta una función de parcialización en la señal legible por una computadora.

50. La señal legible por una computadora de acuerdo con la reivindicación 48, en donde un servidor encripta la señal legible por computadora.

51. Una señal combinada, que comprende:
una señal interior; y

una señal exterior, en donde la señal interior la crea un servidor de autenticación y la señal exterior la crea un servidor protector de compuerta.

52. La señal combinada de acuerdo con la reivindicación 51, en donde la señal interior comprende:

- (a) datos que indican la hora a la cual se creó la señal interior;
- (b) datos que representan un usuario para el cual se creó la señal interior; y
- (c) datos únicos que identifican la señal interior.

53. La señal combinada de acuerdo con la reivindicación 51, en donde la señal exterior comprende:

- (a) datos que identifican a la señal exterior;
- (b) datos que indican la hora a la cual se creó la señal exterior; y
- (c) datos que indican el período de tiempo durante el cual la señal exterior es válida.

54. La señal combinada de acuerdo con la reivindicación 51, en donde un servidor de autenticación firma digitalmente la señal interior.

55. La señal combinada de acuerdo con la reivindicación 51, en donde el servidor de autenticación encripta la señal interior.

56. La señal combinada de acuerdo con la reivindicación 51, en donde el servidor protector de compuerta ejecuta una función de parcialización en la señal combinada.

57. La señal combinada de acuerdo con la reivindicación 51, en donde el servidor protector de compuerta encripta la señal combinada.

58. La señal combinada de acuerdo con la reivindicación 52, en donde los datos que indican la hora a la cual se creó la señal interior se utilizan para determinar si la señal interior es válida.

59. La señal combinada de acuerdo con la reivindicación 53, en donde los datos que indican la hora a la cual se creó la señal exterior se comparan con la hora real para determinar si la señal exterior es válida.

60. El método de autenticar un usuario de acuerdo con la reivindicación 1, en donde la señal de autenticación es menor o igual a 2 kilobytes.

61. El sistema de autenticación de acuerdo con la reivindicación 24, en donde la señal de autenticación es menor o igual a 2 kilobytes.

62. El método de autenticar un usuario de acuerdo con la reivindicación 31, en donde la señal de autenticación es menor o igual a 2 kilobytes.

63. La señal legible por computadora de acuerdo con la reivindicación 42, en donde la señal legible por computadora es menor o igual a 2 kilobytes.

64. La señal combinada de acuerdo con la reivindicación 51, en donde la señal combinada es menor o igual a 2 kilobytes.

65. La señal combinada de acuerdo con la reivindicación 51, en donde la señal interior es menor o igual a 2 kilobytes.

RESUMEN DE LA INVENCION

Un sistema tal como un sistema de computadoras conectadas en red que comprende un usuario, un servidor de aplicación, un servidor protector de compuerta y un servidor de autenticación. El servidor protector de compuerta administra el sistema, en donde el usuario se comunica con el servidor de autenticación y el servidor de aplicación a través del servidor protector de compuerta. Una vez que el servidor de autenticación ha autenticado inicialmente al usuario, el usuario puede solicitar servicios de aplicación de una pluralidad de servidores de aplicación dentro del sistema de computadoras conectadas en red sin tener que ser reautenticado.

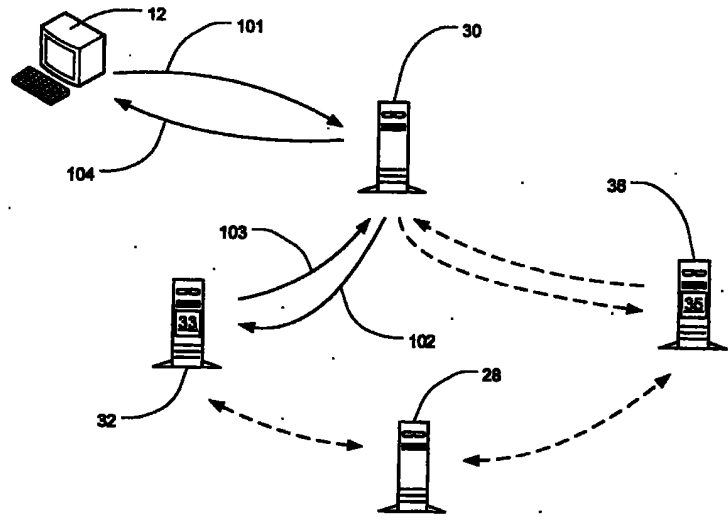


Fig. 1

65

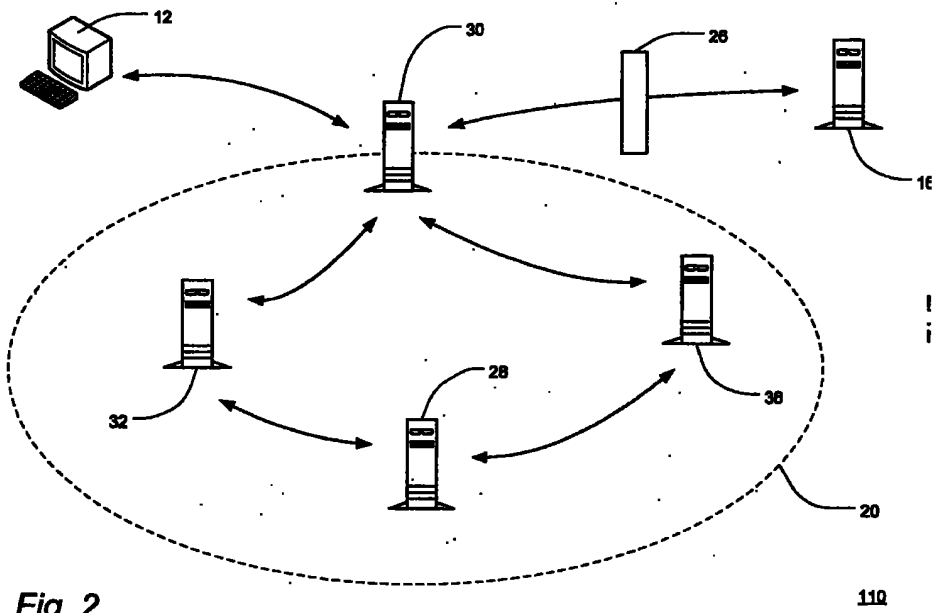
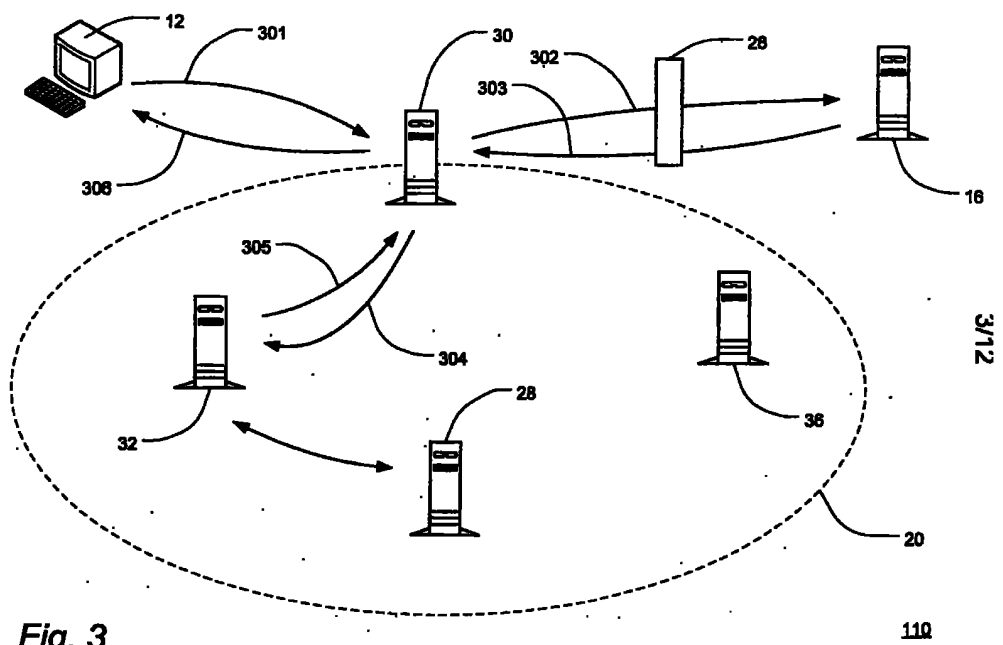


Fig. 2



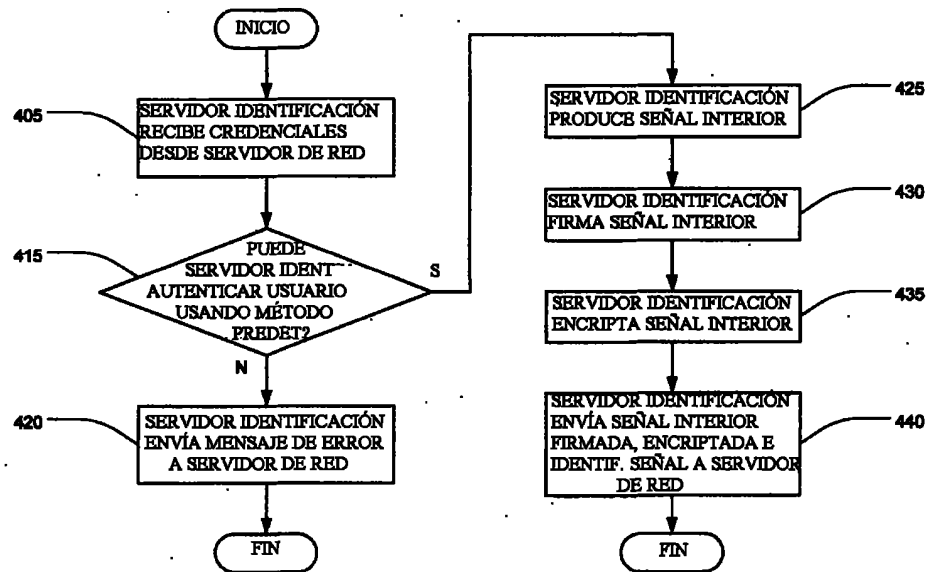


Fig. 4

50

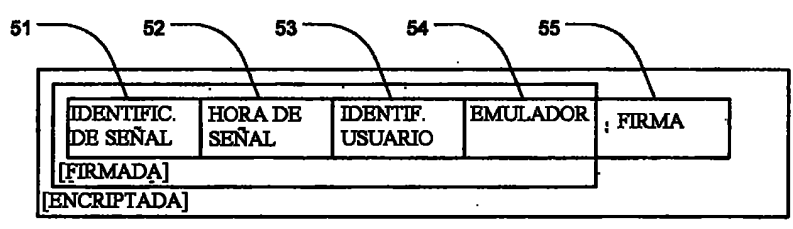


Fig. 5

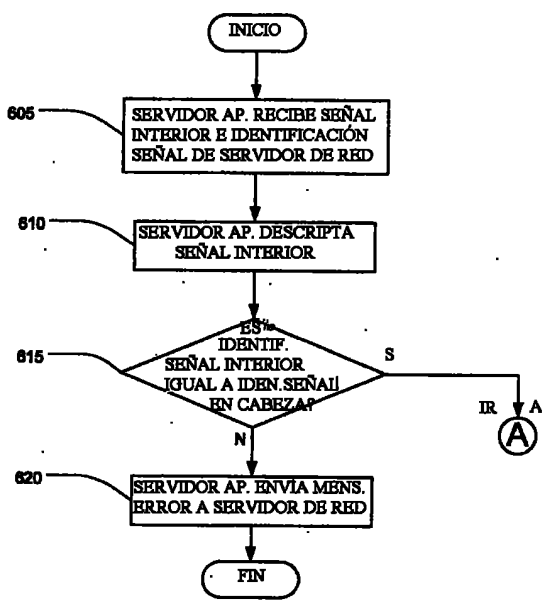


Fig. 6A

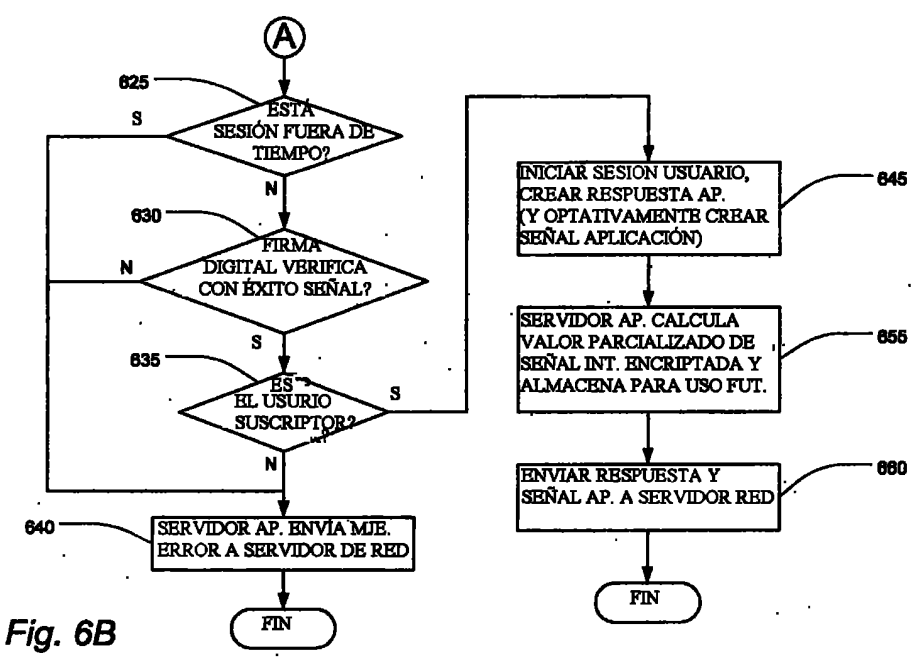


Fig. 6B

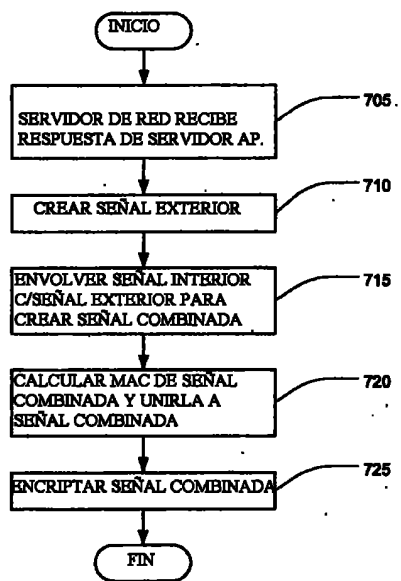


Fig. 7

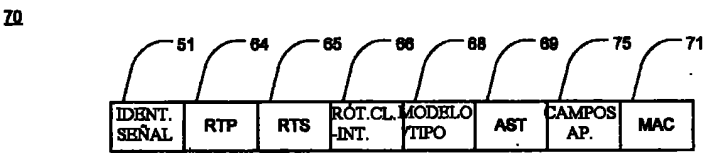


Fig. 8A

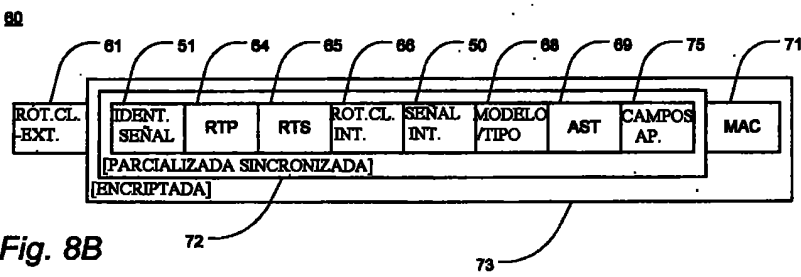


Fig. 8B

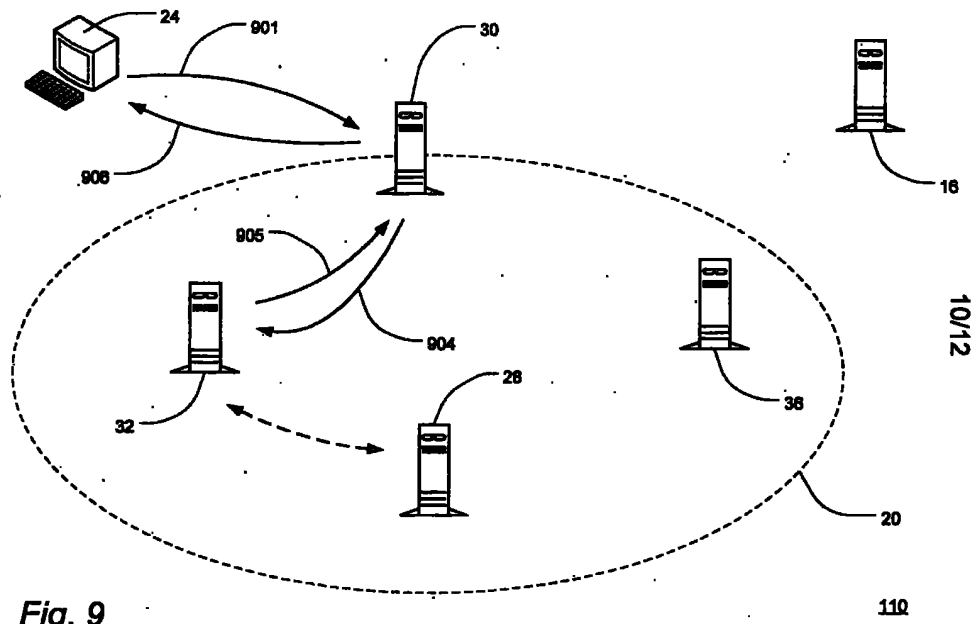


Fig. 9

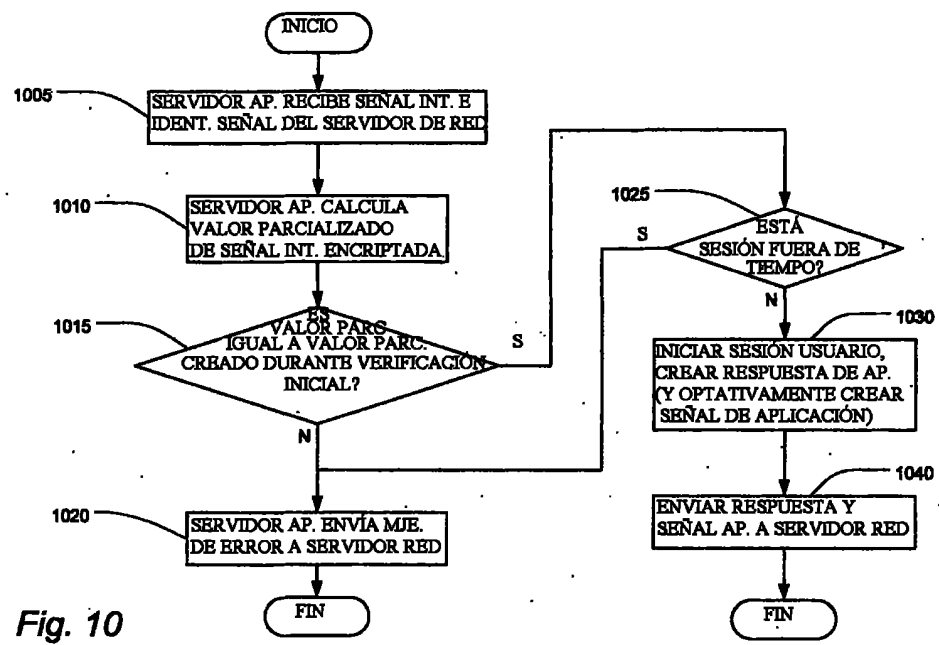


Fig. 10

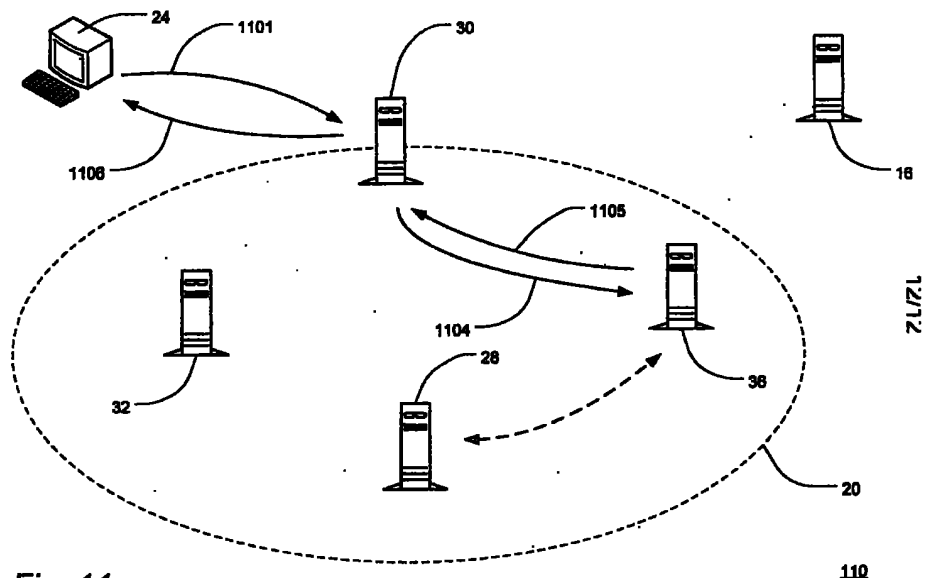
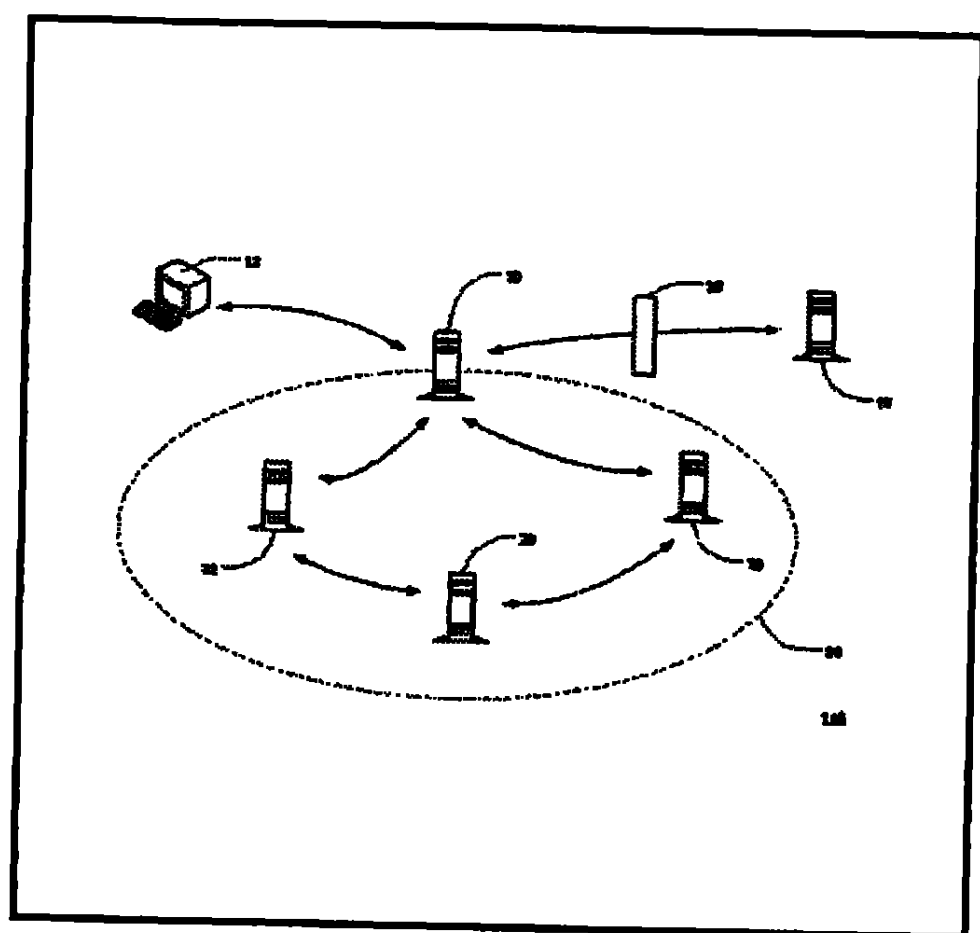


Fig. 11

28

7/15



(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
14 July 2005 (14.07.2005)

PCT

(10) International Publication Number
WO 2005/062989 A2

(51) International Patent Classification: Not classified

(31) International Application Number:
PCT/US2004/043755

(22) International Filing Date:
22 December 2004 (22.12.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/531,695 23 December 2003 (23.12.2003) US

(71) Applicant (for all designated States except US): WA-
CHOVIA CORPORATION [US/US]; 201 South College
Street, Charlotte, NC 28288 (US).

(72) Inventors; and

(75) Inventor/Applicants (for US only): KELLY, Edward,
R. [US/US]; 1289 Centennial Drive, Rock Hill, SC 29732
(US). HOWSER, Christopher, Wayne [US/US]; 1842

Park Grove Place NW, Concord, NC 28027 (US). SAV-
AGE, Jonathan, Francis [GB/US]; 1001 Lampkin Way,
Charlotte, NC 28269 (US). ZHENG, Yaliang [AU/US];
3122 Bridle Brook Way, Charlotte, NC 28270 (US).

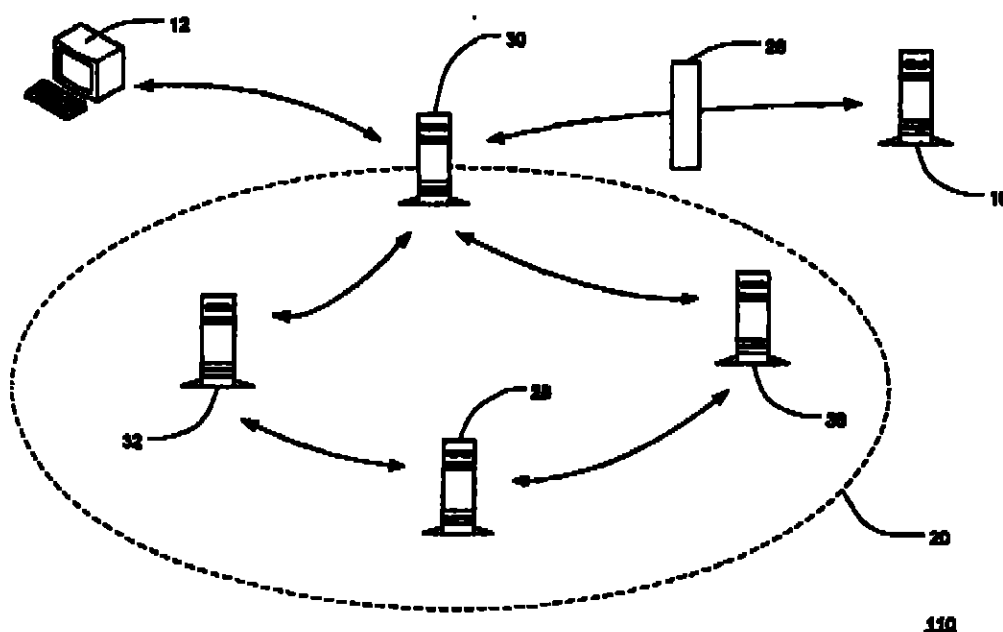
(74) Agent: JACKSON, Susan, S.; Kennedy Covington Lob-
dell & Hickman, LLP, Housat Tower, 47th Floor, 214 North
Tryon Street, Charlotte, NC 28202 (US).

(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN,
CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI,
GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,
KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD,
MG, MK, MN, MW, MX, MZ, NA, NL, NO, NZ, OM, PG,
PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM,
ZW.

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,
ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

(54) Title: AUTHENTICATION SYSTEM FOR NETWORKED COMPUTER APPLICATIONS



(57) Abstract: A system such as in a networked computer system comprising a user, an application server, a gatekeeper server and an authentication server. Communication within the system is managed by the gatekeeper server, wherein the user communicates with the authentication server and the application server through the gatekeeper server. Once the user has been initially authenticated by the authentication server, the user may request application services from a plurality of application servers within the networked computer system without having to be re-authenticated.

WO 2005/062989 A2

29

WO 2005/062989 A2



European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO,
SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN,
GW, ML, MR, NE, SN, TD, TO);

— of inventorship (Rule 4.17(iv)) for US only

Published:

— without international search report and to be republished
upon receipt of that report

Declarations under Rule 4.17:

- of inventorship (Rule 4.17(iv)) for US only
- of inventorship (Rule 4.17(iv)) for US only
- of inventorship (Rule 4.17(iv)) for US only

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

80

**REQUISITOS MINIMOS PARA ADMISION A TRAMITE
PCT**

PATENTE DE INVENCION

[X]

MODELO DE UTILIDAD []

- ◆ Indicación de que se solicita la concesión de una patente [X]
- ◆ Datos de identificación del solicitante o de la persona que presenta la solicitud [X]
- ◆ Descripción de la invención [X]
- ◆ Dibujos de ser estos pertinentes [X]
- ◆ Comprobante de pago de las tasas establecidas [X]

COMPLETA []

INCOMPLETA []

DISEÑO INDUSTRIAL []

- ◆ Indicación de que se solicita el registro de Diseño Industrial []
- ◆ Datos de identificación del solicitante o de la persona que presenta la solicitud []
- ◆ Representación gráfica y fotográfica del Diseño Industrial o muestra del material que incorpora el diseño []
- ◆ Comprobante de pago de las tasas establecidas []

COMPLETA []

INCOMPLETA []

ESQUEMA DE TRAZADO []

- ◆ Indicación de que se solicita el registro de un Esquema de Trazado []
- ◆ Datos de identificación del solicitante o de la persona que presenta la solicitud []
- ◆ Representación gráfica del esquema trazado []
- ◆ Comprobante de pago de las tasas establecidas []

COMPLETA []

INCOMPLETA []


Firma Responsable

Fecha **21 JUN 2006**

Carrera 13 No 27-00 Piso 5 7 y 10
Conmutador 3 82 08 40
Fax 350 52 20
E-mail info@sic.gov.co
www.sic.gov.co
Bogotá D C Colombia

81

REPUBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCI

Bogotá,
2020

Doctor(a)
MAYA RODRIGUEZ CARLOS ORLANDO

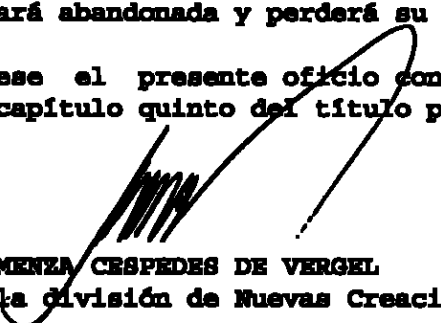
REFERENCIA	Radicación No.	6 60188
	Solicitud internacional	US2004/043755
	Fecha inicio fase nacional	24/07/2006
	Trámite	11
	Evento	379
	Actuación	430
	Oficio No.	7742

Como resultado del examen de forma, realizado con fundamento en el artículo 38 de la Decisión 486 de la Comisión de la Comunidad Andina, artículo 27 del Tratado de Cooperación en Materia de Patentes (PCT), regla 51 bis del Reglamento y Circular Única de la Superintendencia de Industria y Comercio, se le comunica que:

1. Si fuere el caso, el solicitante debe adjuntar la traducción de los anexos del reporte de examen preliminar internacional (Art. 36.2.b) del tratado PCT.
2. La solicitud no contiene la copia del documento en que consta la cesión del derecho a la patente del inventor al solicitante o a su causante. (Art. 26-k) Decisión 486.
3. La solicitud no contiene el poder debidamente otorgado, con el lleno de los requisitos exigidos por los artículos 63 y subsiguientes del Código de Procedimiento Civil. Adicionalmente, deberá presentar el documento que acredita la existencia y representación legal de la sociedad solicitante, cuando ésta fuere persona jurídica.

En cumplimiento de lo dispuesto por el artículo 39 de la Decisión 486, se le requiere para que dentro del término de dos meses siguientes a la fecha de notificación del presente oficio, complete los requisitos anteriormente enunciados. En caso de no dar cumplimiento al presente requerimiento, la solicitud se considerará abandonada y perderá su prelación.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 5.2, literal e), del capítulo quinto del título primero de la Circular Unica No.10 de 2001.


ALIX CARMENZA CESPEDES DE VERGEL
Jefe de la división de Nuevas Creaciones

El anterior requerimiento fue notificado por fijación en lista de fecha 21 JUL 2006
adpall