

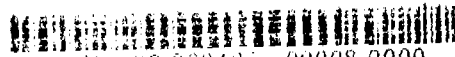
TM TAMAYO & ASOCIADOS
INTERNATIONAL PATENT AND TRADEMARK OFFICE
TECHNOLOGY LICENSING

Technology
Licensing
Trademark
Patent
Health Permit
Design

Transferencia de
Tecnología
Marcas
Patentes
Registros Sanitarios
Diseños

1/32

Señor
JEFE DIVISIÓN DE NUEVAS CREACIONES
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
E. S. I



No. 06-060188-00008-0000

REF: EXPEDIENTE: 06-060188

TITULO: "SISTEMA DE AUTENTICACIÓN PARA
APLICACIONES DE COMPUTADORAS
CONECTADAS EN RED"

ACTUACION: RESPUESTA A EXAMEN DE PATENTABILIDAD

CARLOS ORLANDO MAYA RODRÍGUEZ, mayor de edad, vecino de esta ciudad, identificado con la Cédula de Ciudadanía No.17.117.818 expedida en Bogotá, Abogado titulado en ejercicio y portador de la Tarjeta Profesional No. 17.402 del Consejo Superior de la Judicatura, obrando en calidad de apoderado de la sociedad WACHOVIA CORPORATION. Según poder debidamente conferido y legalizado, adjunto a al expediente de la referencia.

Encontrándome dentro del término legal comparezco para responder el oficio de Requerimiento No. 10940 del Examen de Patentabilidad emanado de esa Oficina, del cual pedimos **prorroga** y con fundamento en el Artículo 45 de la Decisión 486 de 2.000 de C.A.N, damos respuesta en los siguientes términos.

3.- De la solicitud de patente

3.1.- Reivindicaciones

Para atender el requerimiento, según el Artículo 30 de la Decisión 486 se modifica el pliego reivindicatorio, se presenta un nuevo pliego reivindicatorio que se compone de 66 reivindicaciones, con un contenido que se ajusta a los límites impuestos por la memoria descriptiva original, por lo que no exceden el alcance de la invención.

5 - Determinación del estado de la Técnica

En la determinación del estado de la técnica, evaluación del nivel inventivo al hacer referencia a los documentos encontrados con anterioridad, nos permitimos hacer las siguientes aclaraciones respecto a las objeciones formuladas por el Sr. Examinador en cuanto a la falta de novedad de la presente solicitud:

Wood presenta discrepancias con la presente invención. Wood requiere que el PROTECTOR DE COMPUERTA autentique las credenciales del usuario y genere una señal criptográfica. A diferencia, en la presente invención el

servidor de autenticación genera una señal en contraposición al servidor del protector de compuerta. En la presente invención, las credenciales del usuario se autentican en el servidor de registro (servidor de autenticación) y el servidor de registro (servidor de autenticación) genera una señal de autenticación criptográfica.

Wood valida y crea señales en un protector de compuerta que se puede acceder desde el buscador. Esto presenta una desventaja porque el protector de compuerta se encuentra en una posición vulnerable dentro de la arquitectura, por lo tanto, produce una falla en el sistema de seguridad. A diferencia de Wood, en la presente invención la confianza no se deposita completamente en el protector de compuerta. Wood requiere que la señal sea generada por el protector de compuerta, ya que la señal comprende información sobre la caducidad de sesión, que a su vez requiere que la señal sea renovada cada vez que se solicita.

El sistema empleado en la presente invención utiliza dos señales, una de ellas es una señal interna que sirve como señal de autenticación. Su función es autenticar al usuario en el servidor de aplicación y no se renueva. La otra señal es externa y se genera y renueva a través del protector de compuerta. Esta señal de autenticación es el tema de las reivindicaciones que actualmente se encuentran bajo revisión.

Como se mencionó anteriormente, Wood presenta discrepancias con la presente invención porque la función que cumple el protector de compuerta es opuesta a las enseñanzas de la presente invención. El solicitante sostiene, según lo expuesto por Wood, que cualquier compromiso del protector de compuerta permite libre acceso al servidor de aplicación, mientras que en la presente invención el compromiso del servidor del protector de compuerta permite sólo acceso limitado al servidor de aplicación, debido al proceso de verificación que realiza la señal interna. Wood indica que el protector de compuerta brinda acceso a los recursos de información (columna 13, líneas 11-26) una vez que el componente de autorización independiente ha validado el acceso al recurso de información. A diferencia de este, la presente invención transmite sólo la señal de autenticación hacia el servidor de aplicación para que el servidor de aplicación lo evalúe independientemente.

Por lo tanto, la presente invención presenta una característica distintiva en cuanto a la combinación de las referencias citadas en los sistemas de alta disponibilidad o alto rendimiento, gracias a la habilidad de incrementar el número de servidores de Internet, servidores de aplicación o servidores de registro sin aumentar la estructura del mensaje inherente al proceso de sincronización y mantenimiento del estado de la sesión entre una variedad de servidores.

Gupta sostiene que el servidor de aplicación no puede validar una señal sin comunicarse con el servidor de registro. Las señales se validan explícitamente con cada interacción de renovación. Gupta enseña cómo se realiza el almacenamiento en caché para evitar búsquedas múltiples (columna 13, líneas 13- 21). Gupta no enseña o sugiere cómo se pueden renovar las señales si se realiza el almacenamiento en caché. Gupta se basa en el uso de una sesión que se mantiene a través de un servidor (Columna 11, líneas 41- 66). Se accede a esta sesión a través de una clave única que está contenida en el "cookie" del buscador (Columna 11, líneas 62- 66). A diferencia de esta, la presente invención no requiere información de la sesión para funcionar adecuadamente, ya que se realiza una validación criptográfica de la señal para validar la autenticidad de las solicitudes.

El uso de la información de la sesión requiere que todos los servidores puedan acceder al estado de sesión compartido y, por lo tanto, conecten estrechamente todos los servidores a los que se pueden acceder a través del sistema.

El uso de una técnica criptográfica permite controlar el estado de sesión de manera independiente al contexto de autorización. Por lo tanto, la presente invención presenta una ventaja distintiva en cuanto a la combinación de las referencias citadas en los sistemas de alta disponibilidad o alto rendimiento, gracias a la habilidad de incrementar el número de servidores de Internet, servidores de aplicación o servidores de registro, sin aumentar la estructura

6
del mensaje inherente al proceso de sincronización y mantenimiento del estado de la sesión entre una variedad de servidores.

El solicitante sostiene que Wood (Columna 13, líneas 19- 24) no revela un método para autenticar al usuario. Wood simplemente plantea que "las credenciales de registro deben ser suficientes para acceder a la fuente requerida". Los recursos de información no arbitran el acceso del usuario una vez que la solicitud es ingresada en la entrada. En la presente invención el servidor de verificación **corrobor**a la **legitimidad** de la solicitud (a través de la verificación criptográfica) antes de **permitir el acceso**. Wood enseña que las credenciales deben estar protegidas **criptográficamente** durante el tránsito desde el servidor de autenticación **hacia el protector** de compuerta. Por lo tanto, Wood presenta discrepancias con la presente invención.

En la presente invención, el servidor de autenticación crea una señal criptográfica (señal interna) independiente y que no contiene las credenciales de registro. La criptografía utilizada para crear la señal interna se utiliza para establecer una relación de confianza entre el servidor de autenticación y el servidor de aplicación y no para proteger las credenciales. Cuando el servidor de aplicación recibe una señal interna, puede utilizar la clave pública del servidor de autenticación para verificar que la señal se haya emitido a través del servidor de autenticación.

Así, el servidor de aplicación puede tener confianza en la identidad (no las credenciales) de la señal interna. Además, Wood no menciona el motivo por el cual las credenciales están aseguradas criptográficamente y tampoco exige este proceso. Asimismo, no señala el uso de esta información criptográfica. En realidad, Wood plantea explícitamente que la información de la sesión se utiliza para identificar al usuario (Columna 13, líneas 5- 7). No existe el concepto de una relación de confianza entre los servidores de aplicación y el servidor de autenticación excepto el acceso a la red. Los servidores de aplicación pueden ignorar completamente la interceptación de las solicitudes realizadas por el protector de compuerta. Esto presenta discrepancias con la presente invención, en la que el servidor de aplicación interpreta las solicitudes de acceso de manera independiente al protector de compuerta.

Se debe señalar que en Wood se sugiere la firma para que el protector de compuerta pueda validar que la señal no sea manejada por el buscador.

En la presente invención, la firma digital de la señal interna se utiliza para permitir que el servidor de aplicación verifique que el servidor de autenticación evalúe exitosamente las credenciales del usuario. Wood realiza todas las autenticaciones y autorizaciones dentro del servidor que son externas al servidor de aplicación y así descarta la necesidad de la autenticación del usuario para el servidor de aplicación. Esta confianza total del protector de compuerta es un defecto importante. Además, Gupta (Columna 12, líneas 57- 60) no enseña o sugiere la autenticación del usuario pero sí indica la autorización basada en el estado de la sesión. Gupta (Columna 12, líneas 60-

65) enseña que el servidor de aplicación puede acceder al servidor de registro para validar un identificador temporal. Sin embargo, esta técnica no se basa en una relación criptográfica entre el servidor de aplicación y el servidor de registro sino que se centra en las comunicaciones en tiempo real.

Esto requiere comunicaciones directas entre el servidor de registro y el servidor de aplicación, que hace más vulnerable al servidor de registro para atacar la cantidad de caminos de comunicación que existen. También, requiere que el servidor de registro esté disponible. Toda falla del servidor de registro producirá una **falla inmediata de todos los servidores de aplicación** que se basan en él para la **autenticación**. A diferencia de esto, la presente invención no requiere de las comunicaciones en tiempo real, ya que establece relaciones de confianza que requieren un **agresor** para comprometer dos de los tres componentes para actuar en el tercero. Este es un cambio fundamental en la relación entre los distintos componentes porque presenta mayor disponibilidad y seguridad. Por lo tanto, es una ventaja importante en cuanto a la combinación de las referencias citadas.

Gupta (columna 12, líneas 15- 21) no enseña o sugiere cómo el servidor de aplicación autentica al usuario pero sí indica cómo el servidor de aplicación almacena la información que fue autenticada (columna 12, líneas 57-60). Este "cache" requiere comunicaciones en tiempo real entre el servidor de registro y el servidor de aplicación. Además, el servidor de registro tiene que ser conciente de todos los servidores de aplicación y tiene que promover las actualizaciones del servidor. Toda falla o desconfiguración que evite la

9

ejecución de la actualización va a impedir que el usuario acceda al servidor de aplicación. Wood describe una pluralidad de datos dentro de la señal y no una pluralidad de señales.

Cada una de las señales de la presente invención también contienen una pluralidad de datos, pero la pluralidad de señales -cada una protegida criptográficamente de manera independiente- es una distinción importante. La señal que menciona Wood está creada para ser utilizada por la función del protector de compuerta para autenticar, autorizar y direccional solicitudes. Una de las señales de la presente invención se utiliza para el protector de compuerta y la otra para el servidor de aplicación. Esto mantiene la segregación de los servidores, y no se enseña o sugiere a través de la combinación de las referencias citadas. Wood no enseña o sugiere la criptografía como una técnica de autenticación.

Además, sólo se basa en la singularidad de la señal. A diferencia de esto, la presente invención se basa en la relación criptográfica de los componentes y no en los contenidos de datos de la señal. Wood (columna 9, líneas 17-19) no utiliza la criptografía para la autenticación. Esta se basa en una búsqueda de sesión, así como indica Gupta. La criptografía utilizada en la señal es secundaria al enfoque que realiza Wood, que se basa en la identificación de la sesión (línea 17). La criptografía utilizada en Wood ofrece protección para evitar que el usuario (buscador) descifre la señal y no brinda protección contra el compromiso de un componente dentro del sistema. Wood hace referencia a la codificación de una identificación de sesión, pero se utiliza la identificación

de sesión para realizar la autenticación y no la criptografía. Wood señala que no es necesario que el servidor de aplicación esté disponible para decodificar la señal. En realidad, la señal nunca pasa al servidor de aplicación (en Wood llamado "recursos de información"). El protector de compuerta utiliza la señal decodificada como una clave para buscar una sesión.

Gupta no utiliza la criptografía para autenticar al usuario en el servidor de aplicación pero si utiliza comunicaciones en tiempo real (ver arriba). Wood no requiere que la señal esté protegida criptográficamente y, de esta manera, la criptografía no constituye una parte importante del proceso de autenticación.

La identificación de sesión utiliza la autenticación y esto conlleva el problema inherente que se presentó anteriormente. En la reivindicación 24 se describe la relación de confianza importante entre el servidor de aplicación y el servidor de autenticación, que no se enseña o sugiere a través de la combinación de las referencias citadas anteriormente. Mientras que en la reivindicación 6 se caracteriza por presentar un método de validación de la señal como medio de validación de la solicitud.

El sistema de autenticación que menciona Wood se comunica estrictamente con el dispositivo protector de compuerta. La comunicación de red no tiene relación con los servidores de aplicación. Es posible que un mal actor comprometa al protector de compuerta y sobrepase al sistema de autenticación. En la presente invención, la comunicación de red desde el componente de autenticación está diseñada para ser transferida al servidor de

aplicación y para evitar que sea alterada desde el protector de compuerta. Por lo tanto, nuestra reivindicación de la conectividad de red aplica a una serie diferente de relaciones de confianza.

Según Wood el sistema de autenticación describe las comunicaciones generales de Internet que están protegidas por dispositivos de propósitos generales como una barrera de fuego (sistema de protección o "firewall"). Wood claramente presenta un sistema caracterizado porque el dispositivo de protección es un componente de la estructura de seguridad general (protector e compuerta), debido a la necesidad de entender el concepto de Wood sobre una sesión. En la presente invención, existe la posibilidad de que los servidores de autenticación sean segregados por el usuario y otros componentes del sistema sin violar la integridad del método. Esta es una ventaja que presenta el método de la presente invención porque hace posible que los servidores de autenticación residan en una zona de seguridad, un segmento o red diferente que no sean los servidores de protección de compuerta expuestos a Internet y, por lo tanto, poco confiables. Wood requiere la presencia de un servidor de sesión para correlacionar la comunicación entre los distintos componentes.

En cambio, la presente invención no requiere establecer una correlación entre los episodios de comunicación.

El contenido de la señal de la presente invención brinda la información más que la sesión de red. Por lo tanto, la comunicación entre los distintos componentes no está limitada ni controlada por un dispositivo centralizado.

Existe una diferencia entre Wood y la presente invención en cuanto a la naturaleza de la comunicación directa entre el servidor del protector de compuerta y el servidor de aplicación. En Wood el servidor de aplicación se basa completamente en el mensaje transmitido por el protector de compuerta.

Este puede crear sesiones falsas, introducir usuarios que no han suministrado credenciales o exponer a todo el sistema. A diferencia de esto, en la presente invención el protector de compuerta no crea una señal interna y, por lo tanto, no genera sesiones o introduce usuarios que no han suministrado credenciales. En vista de lo anterior, el solicitante respetuosamente pide la reconsideración y se deje sin efecto el rechazo de la presente.

El solicitante reitera la objeción a las consideraciones de Wood y Gupta como se mencionó anteriormente. Las referencias citadas brindan un mecanismo de autenticación del usuario pero ninguna de ellas segrega la funcionalidad para brindar un acceso seguro y un rendimiento mejorado. Wood segrega los componentes pero los correlaciona con el "protector de compuerta" y así hace que "los recursos de información" sean más vulnerables al compromiso. Por su parte, Gupta utiliza un sistema de dos niveles que no se opone al compromiso de ningún componente. A diferencia de esto, la presente

invención brinda una abstracción de la autenticación mientras protege los componentes del sistema. Este concepto es diferente y favorable.

En Wood, el servidor del protector de compuerta brinda funciones múltiples y distintas si se lo compara con el servidor del protector de compuerta, denominado de manera similar, de la presente invención. En Wood, el servidor del protector de compuerta mantiene el estado de la sesión y también coordina las funciones de autenticación y autorización del sistema. En la presente invención, el protector de compuerta sirve para proteger los sistemas internos (función de registro y aplicación) contra preguntas extrañas. La función del protector de compuerta de la presente invención supera las referencias citadas, ya que moderniza la funcionalidad y brinda un mecanismo para los servidores de aplicación para detectar acciones negativas generadas por el protector de compuerta (Párrafos 45 & 48).

A diferencia de la presente invención que limita la autoridad del protector de compuerta, Wood se encuentra obligado a basarse en el protector de compuerta para coordinar los esquemas múltiples de autenticación.

En consecuencia, respetuosamente se solicita reconsideración y abandono del rechazo de la presente. Wood y Gupta permiten una pluralidad de servidores de autenticación, servidores de aplicación y servidores del protector de compuerta. Sin embargo, Wood y Gupta no enseñan ni sugieren la delegación apropiada de claves entre los distintos participantes, y esto es fundamental para el funcionamiento adecuado del sistema. Wood no

considera el concepto de claves compartidas entre el protector de compuerta y los recursos de información.

Gupta no brinda una separación entre el protector de compuerta y el servidor de aplicación. Además, la reivindicación 37 se caracteriza por la relación entre los componentes que no se enseñan o sugieren a través de la combinación de las referencias citadas; mientras que la reivindicación 33 se caracteriza por un método de autenticación del usuario.

Las citadas patentes, entonces, no se constituyen en documentos pertinentes contra la novedad de la presente invención. Consecuentemente, la invención reivindicada en la presente solicitud es novedosa por sobre los documentos citados.

De acuerdo con el nuevo pliego reivindicatorio, la presente invención cumple con los requisitos de patentabilidad exigidos en el Art. 14 de la Decisión 486/2000 de la C.A.N. en el sentido de Novedad, Nivel inventivo y Aplicación Industrial.

Por lo antes expuesto, ruego a usted dar por subsanado dicho requerimiento, sin perjuicio de lo cual desde ya nos acogemos a lo dispuesto por el inciso segundo del artículo 45 de la decisión 486 de la Comunidad Andina de Naciones que a la letra dice: "(...) Cuando la oficina nacional competente estimare que ello es necesario para los fines del examen de patentabilidad, podrá notifica al solicitante dos o más veces (...)" (Subrayado para destacar).

NOTIFICACIONES

Mi poderdante y yo recibiremos notificaciones en la Secretaria de su Despacho o en mi Oficina de Abogado ubicada en la Carrera 13A No. 28-38 Ofc. 246 MZ. 2 Parque Central Bavaria de la ciudad de Bogotá D.C.

Del señor Jefe,



CARLOS ORLANDO MAYA RODRIGUEZ

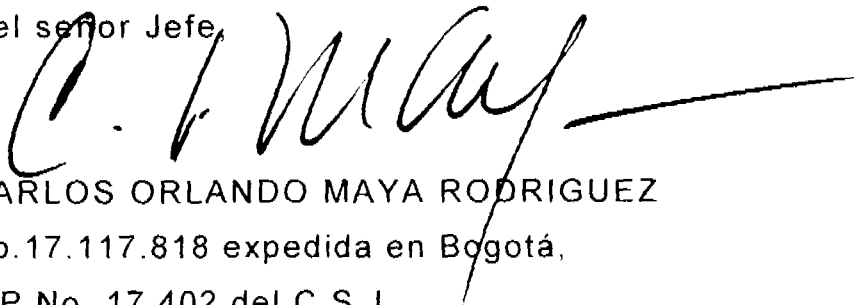
No.17.117.818 expedida en Bogotá,

T.P No. 17.402 del C.S.J.

NOTIFICACIONES

Mi poderdante y yo recibiremos notificaciones en la Secretaría de su Despacho o en mi Oficina de Abogado ubicada en la Carrera 13A No. 28-38 Ofc. 246 MZ. 2 Parque Central Bavaria de la ciudad de Bogotá D.C.

Del señor Jefe,



CARLOS ORLANDO MAYA RODRIGUEZ

No. 17.117.818 expedida en Bogotá,

T.P No. 17.402 del C.S.J.

326
677

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 para identificar únicamente al usuario, la señal de autenticación es independiente de las credenciales del usuario presentadas por el usuario y verificables sin necesidad por parte del usuario de representar dichas credenciales de 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.

17
327
2

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 mediante el servidor de aplicación que la señal de autenticación fue creada por el servidor 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, en donde, la clave de encriptación no es conocida por el servidor protector de compuerta o el usuario.

19
329
136

11. El método de autenticar un usuario de acuerdo con la reivindicación 10, que además comprende desencriptar 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 usando una clave o un par de claves conocidas solamente para el servidor protector de compuerta para formar una señal combinada y retornar la señal combinada al usuario.

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

21
331
137

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 para identificar únicamente al usuario, en donde la señal de autenticación es independiente de las credenciales del usuario presentadas por el usuario y, la señal de autenticación es utilizada por el servidor para verificar que

22
332
113

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.

25
333
74

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 para identificar únicamente al usuario, la señal de autenticación es independiente de las credenciales del usuario presentadas por el usuario y verificables sin necesidad por parte del usuario de representar dichas credenciales de 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 pero no con el usuario; 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;
- (d) un usuario; y
- (e) 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 o el usuario.

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 40, 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

28
338

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. Un sistema de computación en red, que comprende:
un servidor de autenticación,
un servidor protector de compuerta,

un servidor de aplicación, y
una señal combinada legible por computadora, que comprende:
una señal interior; y una señal exterior, en donde la señal
interior es creada mediante el servidor de autenticación y
encriptada por el servidor de autenticación usando una clave
cuya correspondiente clave de desencriptación no se conoce en
el servidor protector de compuerta y, en donde, la señal
exterior es creada mediante el servidor protector de compuerta
y envuelta alrededor de la señal interior para crear la señal
combinada, y la señal combinada encriptada por el servidor
protector de compuerta usando una clave que no es compartida
con el servidor de aplicación y el servidor de autenticación.

52. El sistema de computación en red de 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. El sistema de computación en red de la reivindicación 51,
en donde la señal exterior comprende:

- (a) datos que identifican a la señal exterior;

30
349
111

(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. El sistema de computación en red de la reivindicación 51, en donde un servidor de autenticación firma digitalmente la señal interior.

55. El sistema de computación en red de la reivindicación 51, en donde el servidor protector de compuerta ejecuta una función de parcialización en la señal combinada.

56. El sistema de computación en red de la reivindicación 51, en donde el servidor protector de compuerta encripta la señal combinada.

57. El sistema de computación en red de 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.

58. El sistema de computación en red de la reivindicación 53, en donde los datos que indican la hora a la cual se creó la

31
341
103

señal exterior se comparan con la hora real para determinar si la señal exterior es válida.

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

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

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

62. 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.

63. El sistema de computación en red la reivindicación 51, en donde la señal combinada es menor o igual a 2 kilobytes.

64. El sistema de computación en red de la reivindicación 51, en donde la señal interior es menor o igual a 2 kilobytes.

32
342
23

65. El método de autenticar un usuario de la reivindicación 14, en donde el usuario retorna la señal combinada al servidor protector de compuerta.

66. El método de autenticar un usuario de la reivindicación 65, que además comprende: desencriptar la señal combinada mediante el servidor protector de compuerta, evaluar la señal de salida mediante el servidor protector de compuerta, y pasar la señal de autenticación al servidor de aplicación.

**SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
DIRECCIÓN DE NUEVAS CREACIONES**

Radicación No. 06-60188

Clasificación Internacional (IPC): H04L 29/06

Concepto Técnico No. 2376

Como resultado del examen definitivo, realizado con fundamento en el artículo 48 de la Decisión 486 de la Comisión de la Comunidad Andina, se le comunica:

1. Documentos estudiados

Descripción: Folios: 6 a 48 como se radicó inicialmente

Reivindicaciones: Folios: 49 a 63 como se radicó inicialmente
Folios: 326 a 342 memorial del 2008-12-02

Dibujos: Folios: 65 a 77 como se radicó inicialmente

Prioridad: Folio: 1
(23 dic. 2003, US, N° 60/531695).

Rta. del solicitante: Folios: 310 a 342.

2. Objeto de la invención

La presente solicitud se titula "SISTEMA DE AUTENTICACION PARA APLICACIONES DE COMPUTADORAS CONECTADAS EN RED", Folio N° 1.

El objeto de la presente solicitud se relaciona con un sistema y un método para autenticar un usuario en un sistema de red, donde la autenticación de usuario es valida para todos los servidores conectados a la red de autenticación.

De otra parte, el pliego reivindicatorio modificado reclama: un método de autenticar un usuario con un servidor de autenticación en un sistema de computadoras conectadas en red, relacionado en las reivindicaciones 1 a 23, 59, 65 y 66, un sistema de autenticación dentro de un sistema de computadoras conectadas en red, relacionado en las reivindicaciones 24 a 30 y 60, un método de autenticar un usuario dentro de un sistemas de computadoras conectadas en red, relacionado en las reivindicaciones 31 a 36 y 61, un sistema de autenticación dentro de un sistema de computadoras conectadas en red, relacionado en las reivindicaciones 37 a 41, una señal legible por computadora, relacionada en las reivindicaciones 42 a 50 y 62, y un sistema de computación en red relacionado en las reivindicaciones 51 a 58 y 63 a 64.

El objeto de la solicitud definido anteriormente se clasificó en la H04L 29/06; 9/32.

3. De la solicitud de Patente

3.1. Reivindicaciones (artículo 30 D 486)

Como respuesta al Oficio No. 10940, el solicitante modificó el capítulo reivindicatorio. Sin embargo las modificaciones realizadas no solventan las

objecciones planteadas principalmente porque estas nuevas reivindicaciones tampoco definen ni un producto ni un procedimiento que se ajuste a los lineamientos legales vigentes.

El capítulo modificado reclama básicamente los mismos elementos del capítulo inicial pero hace mayor énfasis en elementos no técnicos tales como señales de comunicación. Igualmente reclama un sistema de computación en red, el cual es exactamente el mismo sistema de computadoras conectadas en red de las reivindicaciones 24 a 30 y el mismo sistema de autenticación dentro de un sistema de computadoras conectadas en red de las reivindicaciones 37 a 41.

Por consiguiente, se ratifican las objeciones planteadas en el Oficio No. 10940 en cuanto:

Las reivindicaciones 1 a 23 y 31 a 36, se refieren a métodos de autenticación de usuario los cuales NO han sido definidos por medio de características técnicas, sino por medio de instrucciones para el procesamiento de datos y señales, lo cual claramente no puede definir un método patentable.

Las reivindicaciones 24 a 30, no define el sistema que se pretende proteger. Una reivindicación de producto debe establecer claramente las relaciones funcionales o estructurales que existen entre los componentes del producto, en este caso del sistema. En lugar de esto, las reivindicaciones calificadas se enfocan en caracterizar el sistema por medio del software que ejecuta un servidor y las señales que el sistema procesa.

El uso de un programa de cómputo o las instrucciones o señales que se procesan en un servidor, son elementos ajenos a la estructura física de un sistema de manera que NO pueden considerarse características técnicas válidas para definir un producto patentable.

Las reivindicaciones 37 a 41 y 51 a 58 se refieren a sistemas definidos exactamente igual al sistema de la reivindicación 24, dado que tales sistemas comprenden exactamente las mismas características:

- Un servidor de aplicación.
- Un servidor protector de compuerta.
- Un servidor de autenticación

Ninguna de los grupos de reivindicaciones indica como es la configuración de los anteriores elementos de manera que técnicamente son iguales. Cabe resaltar que elementos tales como un usuario, señales, claves, datos, etc., NO son elementos técnicos, por lo cual no pueden tomarse en cuenta a la hora de evaluar la invención.

Finalmente se tiene que las reivindicaciones 42 y 51, se refieren a una señal legible por computadora y a una señal combinada respectivamente. Una señal que contiene material descriptivo funcional no es ni un proceso ni un producto, por el contrario, la señal es una forma de energía, que no tiene estructura física ni materia tangible, de manera que sobre tal elemento, no puede reclamarse protección alguna.

Por los motivos anteriores, el pliego reivindicatorio calificado no cumple los requisitos de claridad y concisión exigidos en el artículo 30 de la Decisión 486.

4. No es una invención (artículo 15 D 486)

Las reivindicaciones 1 a 23 del pliego modificado, se refieren a un método de autenticación de un usuario con un servidor en un sistema de computadoras. Como se puede ver las características reclamadas en tales reivindicaciones corresponden a instrucciones para la creación de una señal de autenticación, la cual es procesada por el servidor de autenticación.

Lo anterior corresponde a un procesamiento lógico de instrucciones tal como el que se describe en el algoritmo presentado en la figura 4, que al ser implementado en un sistema de computadoras, hace que este sistema realice determinada tarea u obtenga un determinado resultado. Esto es soporte lógico como tal, lo cual no se protege por patente de acuerdo a lo establecido en el literal e) del artículo 15.

El método reclamado en la reivindicación 31 y sus dependientes, presenta las mismas características que el método de la reivindicación 1, por lo tanto la materia reclamada en estas reivindicaciones también se trata de soporte lógico como tal.

El pliego reivindicatorio se enfoca en describir la creación, utilización y la información contenida en señales de autenticación. Una señal de comunicación no es un elemento físico sino un portador de información de manera que la definición de la señal esta dada en términos de la información contenida en esta, lo cual claramente es presentación de información.

De acuerdo a lo anterior, las características presentadas en el pliego no son validas toda vez que tanto los método como los sistemas reclamados fueron definidos en función de señales de comunicación, es decir que las características esenciales de los objetos reclamados, se tratan de presentación de información, lo cual no puede considerarse una invención de acuerdo a lo establecido en el literal f) del artículo 15.

La no patentabilidad del pliego se aprecia fácilmente al observar la materia reclamada en la reivindicación 42 y sus dependientes, donde la señal legible por computadora, esta caracterizada por un primer nodo de datos "*que comprende datos que identifican la estructura de datos*", y un segundo nodo de datos "*que comprende datos que indican la hora*". Es muy claro que la señal esta definida por medio de los datos contenidos en esta.

De acuerdo a los literales e) y f) del Art. 15, lo que se reclama en el pliego calificado NO puede considerarse una invención.

5. Determinación del Estado de la Técnica

Considerando que la solicitud reclama prioridad del 23 de diciembre del 2003, se buscaron documentos del estado de la técnica relacionados, con fecha de publicación anterior a esta. Se realizo búsqueda de documentos relevantes dentro del estado de la técnica, entendiendo como estado de la técnica la definición provista en el Art. 16 D 486, y las excepciones fijadas en el Art. 17 de la misma.

Se encontró como anterioridades los documentos relacionados a continuación que afectan la patentabilidad del objeto de la presente solicitud

N°	Documento	Título	Fecha de publicación
D1	US6609198	LOG-ON SERVICE PROVIDING CREDENTIAL LEVEL CHANGE	2003-08-19

		WITHOUT LOSS OF SESSION CONTINUITY	
D2	US2001/0037469	METHOD AND APPARATUS FOR AUTHENTICATING USERS	2001-10-01

6. Análisis de patentabilidad (artículo 14 D486)

En cumplimiento del Art. 14 D486 se procedió a evaluar los requisitos de novedad, nivel inventivo y aplicabilidad industrial, con el fin de establecer la patentabilidad de la invención reivindicada de la solicitud en estudio.

6.1. Novedad (artículo 16 D486)

El requisito de novedad se evaluó mediante la comparación entre la materia reclamada y los documentos encontrados en el estado de la técnica. Como el documento no presenta características técnicas para definir la invención, se procedió a realizar una simple comparación entre los componentes que comprenden los sistemas reclamados, con los sistemas del estado del arte.

La reivindicación 24 se refiere a un sistema de autenticación dentro de un sistema de computadoras que comprende lo siguientes elementos:

- Un servidor de aplicación.
- Un servidor de autenticación.

La anterioridad **D1**, se refiere a una arquitectura de seguridad que permite especificar un único esquema de identificación válido para múltiples fuentes de información. La arquitectura presentada en este documento contempla una aplicación de búsqueda **170**, y un componente de autenticación **130** (ver Fig. 1). Como puede verse este documento contempla todas las características definidas en la reivindicación.

La anterioridad **D2** la cual se refiere a un método y un aparato para la autenticación de usuarios, contempla un servidor de aplicación **202**, en comunicación con un servidor de autenticación **204** (Fig. 2), de tal forma que este documento también contiene todas las características presentadas en la reivindicación 24.

La reivindicación 25, se refiere a una conexión entre el servidor de autenticación y las computadoras en red. La anterioridad **D2**, muestra una línea de comunicación directa **206**, entre el servidor de autenticación **202** y el usuario **200**. De igual manera el documento **D1** muestra comunicación entre el componente de autenticación **130** y la red de fuentes de información **190**.

Las reivindicaciones 26 a 28 especifican un servidor protector conectado con el servidor de aplicación y el servidor de autenticación. La anterioridad **D1** muestra que el componente de autenticación **130** interactúa con el buscador **170** vía un dispositivo de protección **110** (servidor protector). De manera que las características especificadas en estas reivindicaciones tampoco son nuevas.

La reivindicación 29 especifica que el servidor de autenticación recibe comunicación solamente desde el servidor protector. En la figura 1 del documento **D1** se ve que la comunicación entre el elemento de autenticación **130** con la aplicación de búsqueda **170**, se realiza únicamente a través del servidor protector **110**. Por lo cual esta característica tampoco es nueva.

Cabe recalcar que la mayor parte de la exposición se refiere a las características de una señal de comunicación, sobre lo cual no se evalúa la novedad, dado que la señal no corresponde a materia técnica. Igualmente la reivindicación reclama un usuario como parte de la invención, lo cual no es aceptable por cuanto el sistema es independiente de cómo se use y de quien lo use.

La reivindicación 37 y sus dependientes, y la reivindicación 51 y dependientes, se refieren a sistemas definidos por los mismos elementos presentados en las reivindicaciones 24 a 30, por lo cual los objetos reclamados en estas reivindicaciones tampoco son nuevos.

En conclusión, al hacer la comparación elemento por elemento entre lo solicitado y el estado de la técnica, se encuentra que las características esenciales del objeto de esta solicitud son idénticas a lo comprendido en los documentos D1 y D2, razón por la cual la solicitud no cumple con los requisitos de novedad establecidos en el artículo 16 de la Decisión.

7. Respuesta a los argumentos del solicitante:

7.1. Reivindicaciones

El pliego reivindicatorio modificado fue aceptado y se calificó arriba en el punto 3, acorde a las disposiciones y el procedimiento vigentes.

7.2. Determinación del estado de la técnica

En defensa de la patentabilidad del método reclamado, el solicitante señala algunas consideraciones en relación con la novedad de la solicitud.

El solicitante señala diferencias entre la presente solicitud y el estado de la técnica pero como se mostrará a continuación las diferencias señaladas no son de carácter técnico, sino que obedecen a diferencias en el software y el procesamiento de señal:

"A diferencia, en la presente invención el servidor de autenticación genera una señal en contraposición al servidor del protector de compuerta"

"A diferencia de Wood, en la presente invención la confianza no se deposita en el protector de compuerta"

"El sistema empleado en la presente invención utiliza dos señales."

"A diferencia de este, la presente invención transmite solo la señal de autenticación hacia el servidor de aplicación para que el servidor de aplicación lo evalúe independientemente"

"la presente invención presenta una característica distintiva en cuanto a la combinación de las referencias citadas en los sistemas de alta disponibilidad o alto rendimiento, gracias a la habilidad de incrementar el número de servidores de Internet..."

"Gupta no enseña o sugiere como se pueden renovar las señales si se realiza el almacenamiento en caché... A diferencia de esta, la presente invención no requiere información de la sesión para funcionar adecuadamente, ya que se realiza una validación criptográfica de la señal para validar la autenticidad de las solicitudes"

“El uso de una técnica criptográfica permite controlar el estado de sesión de manera independiente al contexto de autorización.”

“En la presente invención, el servidor de autenticación crea una señal criptográfica (...) independiente y que no contiene las credenciales de registro.”

Etc.

Como se puede ver el solicitante no presenta ningún argumento técnico a favor de la novedad de la solicitud. El manejo de señal, la encriptación de códigos, o la programación de dispositivos de procesamiento tal como servidores, NO son característicos de orden técnico que permitan definir una invención tal como la que se pretende proteger.

Como se dijo en comunicaciones anteriores, la definición de un sistema que se pretenda patentar, debe realizarse por medio de sus componentes y las relaciones funcionales o estructurales existentes entre los mismos. El documento de la referencia no indica ningún circuito, forma de conexión o de acople entre los componentes del sistema reclamado, ya que todo el sistema fue definido en términos del uso de software y procesamiento de señal. Por lo anterior es claro que la presente solicitud no corresponde a una invención. Igualmente es claro que un sistema compuesto por servidores tal como el que se presenta, NO es un sistema nuevo, sino que este es un sistema ampliamente conocido que presenta muchas funcionalidades tal como el solicitante argumenta en su respuesta.

7.3. No es una invención

El solicitante no presento argumentos en contra de las objeciones planteadas respecto a este punto.

En consecuencia y por todo lo expuesto anteriormente, se recomienda **Negar** las reivindicaciones: 1 a 66 (folios: 326 a 342).

Bogotá, D.C.,

CONCEPTO TECNICO No. 2376	EXAMINADOR TECNICO Código No. 202082
---------------------------	---