

TM TAMAYO & ASOCIADOS
INTERNATIONAL PATENT AND TRADEMARK OFFICE

Patentes
Patentes
Registros Sanitarios
Soporte Lógico
Nombres Comerciales
Diseños

Marcas
Patentes
Registros Sanitarios
Soporte Lógico
Nombres Comerciales
Diseños

Señores
SUPERINTENDENCIA DE INDUSTRIA Y CO
DIVISIÓN DE NUEVAS CREACIONES
E. S. D.

MINISTERIO DE INDUSTRIA Y COMERCIO



NO. 06-060188-00005-0000

Dep. 2020 NUECREACION
Ley 379 FASENACIONALII
Folios 2

REF: EXPEDIENTE No. 06-060188
SOLICITUD INTERNACIONAL: PCT/US/2004/043755
CAPITULO II
ACTUACIÓN: SOLICITUD DE EXAMEN PATENTABILIDAD

Estimados señores:

Con fundamento jurídico en lo dispuesto por el Artículo (44) de la Decisión (486) de la Comisión de la Comunidad Andina de Naciones (CAN) ruego a ustedes disponer lo pertinente para proceder al Examen de Patentabilidad de la Solicitud citada en la referencia, para lo cual estamos adjuntando el recibo de pago correspondiente a la tasa vigente para este caso.

En consecuencia, esperamos se surta este trámite para que el expediente siga su curso normal, hasta su concesión.

Atentamente,


CARLOS ORLANDO MAYA RODRÍGUEZ.

C.C. No. 17.117.818- Bogotá

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

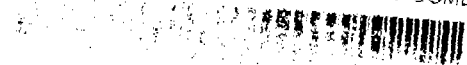
Anexo.- Recibo de Pago No.08-

18270

7916

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

MINISTERIO DE INDUSTRIA Y COMERCIO



REGIONAL

NIT : 000171001-1

RECIBO OFICIAL DE PAGO : 08 - 10,270
 CHA : FEBRERO 29 DE 2018

***** COMISIONACION *****

PROPOSITANTE	TIPO PAGO	PAQUETE	CUENTA	NIT PAQUETE	FECHA PAGO	VAL. PAGO
CARLOS TAMAYO Y ASOCIADOS-CONSIGNACION		PAQUETE DE SERVICIOS	480754387	279300	29/02/2018	250,000.00

***** C O N C E P T O *****

CONCEPTO	VALOR	TOTAL CONCEPTO
1. VALORES DE SOLICITUDES	250,000.00	250,000.00
TOTAL		250,000.00

CON: CIENTO CINCUENTA MIL PESOS

RESPONSABLE: 

RECIBO DE PAGO APLICADO AL EXPEDIENTE No. 06-60188

DIVISIÓN DE NUEVAS CREACIONES

RADICACIÓN EXPEDIENTE No. 06-60188

EL EXTRACTO DE LA PRESENTE SOLICITUD DE **PATENTE DE INVENCION**

FUE PUBLICADO EN LA GACETA DE PROPIEDAD INDUSTRIAL No **584** DE

FECHA **31 DE DICIEMBRE DE 2007** EL TÉRMINO HÁBIL SEÑALADO POR LA

LEY EXPIRA EL **31 DE MARZO DE 2008**

NOTA: Dentro del plazo de los seis (6) meses siguientes a partir de la fecha de publicación en la gaceta de Propiedad Industrial, deberá solicitar y cancelar el examen de patentabilidad so pena de que la solicitud caiga en abandono, de acuerdo con lo establecido en el Artículo 44 de la Decisión 486/2000.

SE PRESENTARON OPOSICIONES POR PARTE DE TERCEROS.

SI _____

NO X



US006609198B1

(12) **United States Patent**
Wood et al.

(10) Patent No.: **US 6,609,198 B1**
(45) Date of Patent: **Aug. 19, 2003**

(54) **LOG-ON SERVICE PROVIDING
CREDENTIAL LEVEL CHANGE WITHOUT
LOSS OF SESSION CONTINUITY**

(75) Inventors: **David L. Wood**, Louisville, CO (US);
Paul Weschler, Broomfield, CO (US);
Derk Norton, Louisville, CO (US);
Chris Ferris, Whitinsville, MA (US);
Yvonne Wilson, Mountain View, CA
(US); **William R. Soley**, Campbell, CA
(US)

(73) Assignee: **Sun Microsystems, Inc.**, Santa Clara,
CA (US)

(*) Notice: Subject to any disclaimer, the term of this
patent is extended or adjusted under 35
U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/368,506**

(22) Filed: **Aug. 5, 1999**

(51) Int. Cl.⁷ **G06F 1/26**

(52) U.S. Cl. **713/155; 713/182; 713/200;**
713/201

(58) Field of Search **713/155, 169,**
713/182, 200, 201

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,826,014 A 10/1998 Coley et al. 395/184,01
5,875,296 A 2/1999 Shi et al. 395/188,01

FOREIGN PATENT DOCUMENTS

EP 0 465 016 A 1/1992
EP 0 849 680 A 6/1998
WO 96/42041 12/1996
WO 98/25373 6/1998
WO 98/57247 12/1998

OTHER PUBLICATIONS

"X-Open Single Sign-On Service (XSSO)—Plugged
Authentication Modules," *Open Group Preliminary Specifi-*
cation, P702 ISBN 1-85912-144-6, Jun. 1997, 140 pages.

(List continued on next page.)

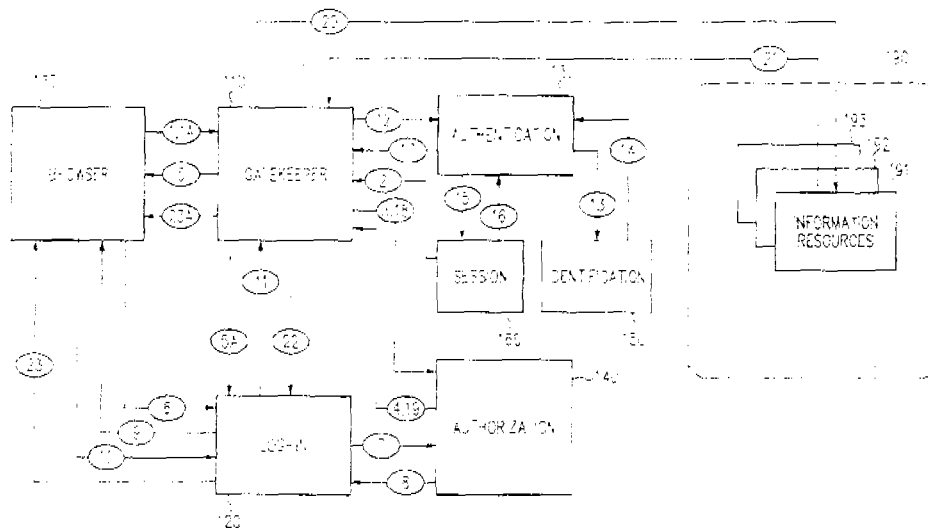
Primary Examiner: Thomas R. Peeso

(74) Attorney, Agent, or Firm—Zagorin, O'Brien &
Graham, LLP

(57) **ABSTRACT**

A security architecture has been developed in which a single
sign-on is provided for multiple information resources.
Rather than specifying a single authentication scheme for all
information resources, the security architecture associates
trust-level requirements with information resources.
Authentication schemes (e.g., those based on passwords,
certificates, biometric techniques, smart cards, etc.) are
employed depending on the trust-level requirement(s) of an
information resource (or information resources) to be
accessed. Once credentials have been obtained for an entity
and the entity has been authenticated to a given trust level,
access is granted, without the need for further credentials
and authentication, to information resources for which the
authenticated trust level is sufficient. The security architec-
ture allows upgrade of credentials for a given session. This
capability is particularly advantageous in the context of a
single, enterprise-wide log-on. An entity (e.g., a user or an
application) may initially log-on with a credential suitable
for one or more resources in an initial resource set, but then
require access to resource requiring authentication at higher
trust level. In such case, the log-on service allows additional
credentials to be provided to authenticate at the higher trust
level. The log-on service allows upgrading and/or down-
grading without loss of session continuity (i.e., without loss
of identity mappings, authorizations, permissions, and envi-
ronmental variables, etc.).

34 Claims, 7 Drawing Sheets



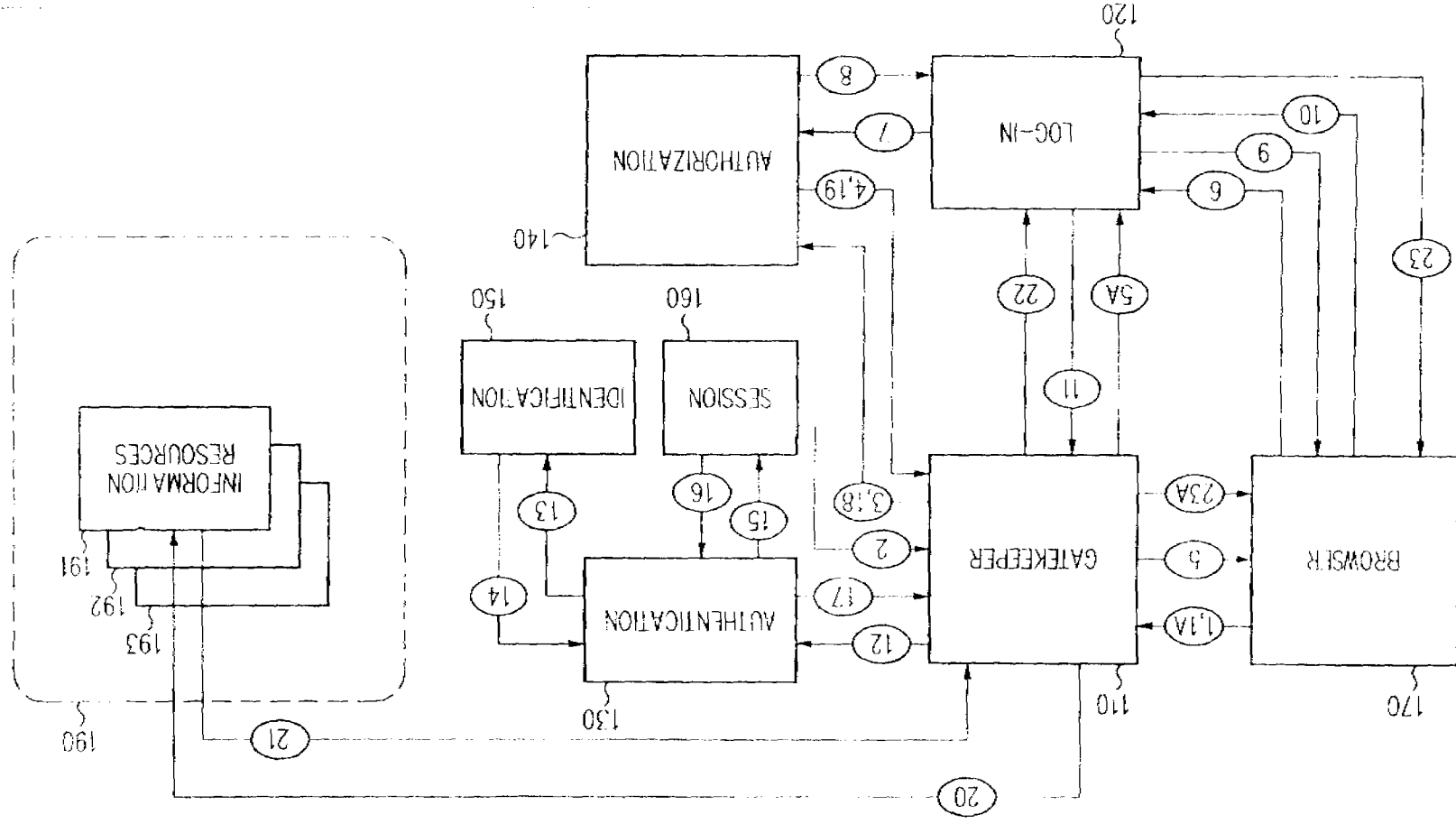


FIG. 1

ificates or other encrypted indicia based on asymmetric, symmetric, public, private, or secret key technologies, one-time passwords, biometric indicia such as by retinal scan, voice print, finger print, etc., and possession based indicia such as smart cards, Enigma cards, keys, etc. In some realizations, credentials may be associated with users, sessions, functional objects, etc.

Digital Signature: A transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key and whether the message has been altered since the transformation was made.

Entity: A user or object, including data objects and/or functional objects such as applications, components, modules, services, processes, threads, etc., as well as instantiations thereof. In some configurations, only user entities (typically, the human principal interacting with a software program or on whose behalf a software agent purports to act) are considered. In other configurations, entities include functional objects without an associated human principal. The identity of an entity may be authenticated using a credential.

Session: A period and collection of states spanning one or more interactions between an entity and an information environment. As used herein a session may span multiple interactions with multiple resources of the information environment and, in some configurations, may span multiple information access protocols (e.g., HTTP, FTP, telnet, etc.). A session has a beginning and an end. During its existence, a session has state. As used herein, the term session connotes a greater persistence than as sometimes used to describe the period of a "session layer" protocol interaction, which in the case of some protocols, such as HTTP, is generally very short-lived.

Single Sign-on Security Architecture

FIG. 1 provides an overview of major interactions between components for an exemplary security architecture in accordance with the present invention. As illustrated in FIG. 1, a client application, e.g., a browser 170 operated by a user, interacts with the security architecture via a gatekeeper and entry handler component 110 and a login component 120. Gatekeeper and entry handler component 110 provides an entry point for external client applications requesting access to enterprise applications and/or resources 190, including e.g., information resources 191, 192, . . . 193, for which access management is provided by the security architecture. Using facilities provided by a session management component 160, an authorization component 140, an authentication component 130, an identification component 150, and login component 120, the gatekeeper entry handler component 110 allows, redirects or refuses access requests in accordance with a security policy.

Individual information resources typically have differing security requirements. In addition, individual types of access to a single information resource may have differing security requirements. Nonetheless, a given level of security may be sufficient for more than one of the information services or access types. For example, information resource 191 may include a product information service for providing general information such as product descriptions or data sheets to the public, while information resource 192 includes an order processing system for an eCommerce site. Information resource 193 may include functions for supply chain interactions such as access to inventory information or current selling price information. Both the product information

service and order intake functions of the eCommerce may operate with similar security requirements, e.g., allowing access by minimally authenticated, non-hostile entities. On the other hand, supply chain functions may require a higher level of security. Order status functions of the order processing system may require a mid-level of security.

Login component 120, operating in conjunction with gatekeeper entry handler component 110 and other components of the security architecture, provides a single sign-on interface for access to enterprise applications and/or resources 190. In an exemplary embodiment, security requirements are expressed in terms of trust levels and login component 120 obtains login credentials for an entity requesting access to one of the enterprise applications and/or resources 190. The login credentials obtained are selected from a set of credential types that, if authenticated, are sufficient to achieve the trust level requirement of an application or information resource to be accessed. Without limitation, typical login credential types and associated authentication mechanisms include those based on passwords, certificates, biometric techniques, smart cards, etc. Other credential types and associated authentication mechanisms are described elsewhere herein.

In some embodiments in accordance with the present invention, gatekeeper entry handler component 110 queries authorization component 140 to obtain authorization for access to a particular requested enterprise application or information resource by the requesting entity (e.g., the browser user). If the entity requesting access has not yet been authenticated to the trust level required for the particular access to the particular enterprise application or information resource requested, authorization component 140 may indicate that the access request is to be redirected to login component 120 so that login credentials may be obtained and authenticated to a particular trust level. If, on the other hand, login credentials have already been obtained for the requesting entity and the requesting entity has been authenticated using the obtained credentials such that the required trust level has been achieved, the access will typically be allowed without the need for further login credentials and authentication. In certain circumstances, authorization component 140 may indicate that the access is to be refused. For example, authorization component 140 may be programmed to perform more stringent testing beyond a trust level requirement. In an exemplary enterprise tool configuration, a desired security policy may dictate that a salary tool is accessible only from within a company's internal network. No level of authenticated trust may be sufficient to access such a tool from outside company network. To facilitate implementation of such a security policy, authorization component 140 could refuse access based on environment parameters indicating a session originating outside the company's internal network.

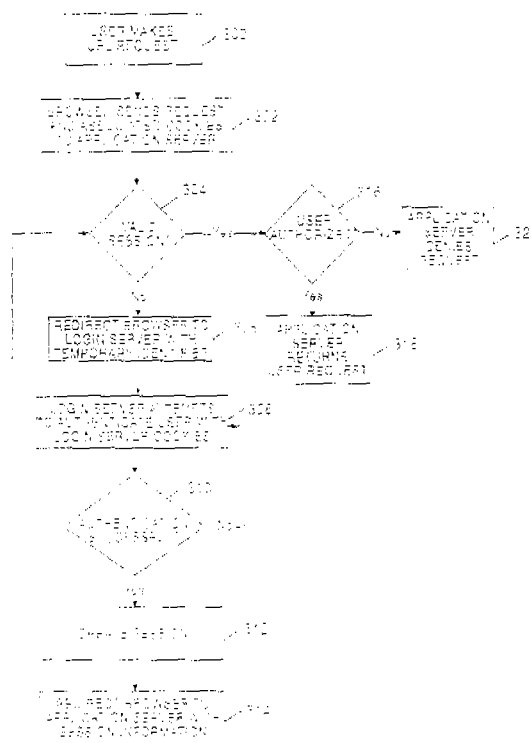
Of note, in certain embodiments in accordance with the present invention, the mapping of login credential types and authentication mechanisms to trust levels is influenced by environment information such as time of request, source of request, connection speed, and/or client application (e.g., browser) environment information. In this way, even with a static set of mapping rules, the set of credential types and authentication mechanisms suitable to support a given trust level may vary based on environment information. In general, mapping rule dependencies are based on perceived variations in threat characteristics and/or requesting entity capabilities. In some embodiments in accordance with the present invention, gatekeeper entry handler component 110 is the authority on environment information for a particular requesting entity.



US 20010037469A1

(19) **United States**(12) **Patent Application Publication****Gupta et al.**(10) **Pub. No.: US 2001/0037469 A1**(43) **Pub. Date:****Nov. 1, 2001**(54) **METHOD AND APPARATUS FOR
AUTHENTICATING USERS**(75) **Inventors:** **Abhay Gupta**, Milpitas, CA (US);
Chris Ferris, Whitinsville, MA (US);
Alejandro Abdelnur, Sunnyvale, CA
(US)**Correspondence Address:****THE HECKER LAW GROUP
1925 CENTURY PARK EAST
SUITE 2300
LOS ANGELES, CA 90067 (US)**(73) **Assignee:** **SUN MICROSYSTEMS, INC.**(21) **Appl. No.:** **09/838,703**(22) **Filed:** **Apr. 18, 2001****Related U.S. Application Data**(65) **Continuation of application No. 09/309,341, filed on
May 11, 1999, now Pat. No. 6,326,752.****Publication Classification**(51) **Int. Cl.⁷** **H04L 9/00; H04L 9/32;
G06F 11/30; G06F 12/14**
(52) **U.S. Cl.** **713/202**(57) **ABSTRACT**

A method and apparatus for authenticating users. Prior art mechanisms require each individual application (running on an "application server") that the user is accessing to provide for the ability to use the various authentication mechanisms. One or more embodiments of the invention externalize the authentication mechanism from the application in the form of a login server. Only the login server needs to be configured to handle authentication mechanisms. The application server checks if a request has an active and valid session (e.g., a valid session may exist when there is active communication between a client and server that has not expired). If there is not a valid session, the application server redirects the user to the login server. The login server attempts to authenticate the user using any desired authentication mechanism. Once authenticated, the login server redirects the user back to the application server. The application server verifies the authentication directly with the login server. Once verified, the application server processes the user's request and responds accordingly. One or more embodiments of the invention may utilize cookies to aid in the authentication process. Thus, applications on the application server need not be concerned about authenticating a given user. The application server merely knows how to work with the login server to authenticate the user. Further, communications between the application server and login server are transparent (or without any interaction from) the user (although the user may see the browser communicating with each server).



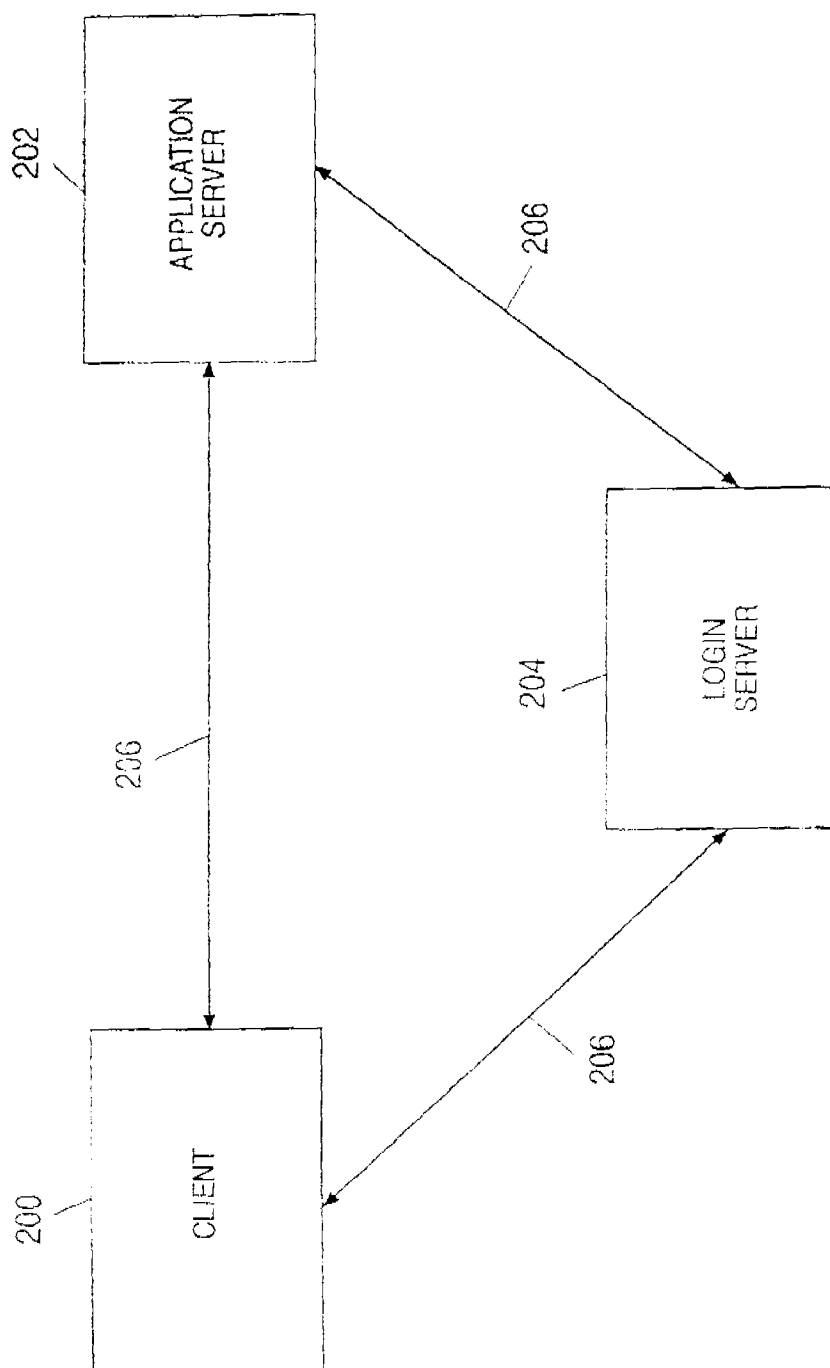


FIGURE 2

303
~~302~~

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
DIVISIÓN DE NUEVAS CREACIONES

2020
Bogotá, D.C.,

Abogado
CARLOS ORLANDO MAYA RODRIGUEZ

ASUNTO	Radicación	06-60188
	Trámite	011
	Evento	378
	Actuación	430
	Oficio	10340
	Folios	011

Patente de Invención ☒ Patente de Modelo de Utilidad ☐

Vía Nacional ☐

Vía PCT (fase nacional) ☒ Cap. I ☒ Cap. II ☐

No. Sol. Internacional PCT/US2004/043755
Fecha de Presentación Internac. 22 de diciembre de 2004

Como resultado del examen de fondo, realizado con fundamento en el artículo 45 de la Decisión 486 de la Comisión de la Comunidad Andina, se le comunica:

1. Documentos estudiados

- 1.1. Descripción: Folios: 6 a 48 como se radicó inicialmente
- 1.2. Reivindicaciones: Folios: 49 a 63 como se radicó inicialmente
- 1.3. Dibujos: Folios: 65 a 77 como se radicó inicialmente
- 1.4. Prioridad: Folio: 1
(23 dic. 2003, US, N° 60/531695).

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 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 y 60, un sistema de autenticación dentro de un sistema de computadoras conectadas en red, relacionado en las reivindicaciones 24 a 30 y 61, un método de autenticar un usuario dentro de un sistemas de computadoras

conectadas en red, relacionado en las reivindicaciones 31 a 36 y 62, 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 63, y una señal combinada, relacionada en las reivindicaciones 51 a 59 y 64 a 65

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)

Las reivindicaciones calificadas no definen la materia que se desea proteger, ya que no presentan ni un producto ni un procedimiento que se ajusten a los lineamientos legales vigentes.

Las reivindicaciones 1 a 23 se refieren a un método de autenticar a un usuario, consistente en las etapas de:

- a) presentar credenciales de usuario.
- b) Proporcionar las credenciales de usuario
- c) Autenticar al usuario
- d) Crear una señal de autenticación
- e) Transmitir la señal de autenticación

Las etapas anteriores no conforman un procedimiento que pueda ser patentable dadas las siguientes razones:

- i) No conlleva a la obtención de un producto tangible, tal como un aparato o una máquina.
- ii) Las etapas presentadas indican la forma de operación (utilización) de un sistema de autenticación.
- iii) No resuelve ningún problema técnico (el problema de autenticación se resuelve con el sistema de autenticación, no con las instrucciones de operación del sistema)
- iv) El método relacionado no corresponde a un proceso industrial, ni hace parte de uno.

De acuerdo a lo anterior, el método mencionado no cumple con los requisitos mínimos para poder considerarse patentable. Igual situación ocurre con el método de las reivindicaciones 31 a 36, que esencialmente es el mismo método anterior pero proporcionando una segunda y una tercera clave de encriptación.

La reivindicación 24 no define la materia que se desea proteger, debido a lo siguiente:

- i) No se define cual es la materia **característica** de la invención, la cual no hace parte del estado del arte.
- ii) La reivindicación se limita a enumerar una serie de componentes tales como un servidor de aplicación y un servidor de autenticación, pero no presenta la relación estructural existente entre estos componentes. Cabe destacar que una red o un sistema de comunicación siempre se debe definir por medio de características estructurales tales como la forma de conexión de los dispositivos (serie, paralelo, serial, inalámbrica, etc.) o los circuitos formados por estos.
- iii) Una señal de autenticación y un usuario no características técnicas de la invención, por lo cual no pueden hacer parte del pliego reivindicatorio.

La reivindicación 25 no especifica como es la comunicación del servidor de autenticación con el sistema de computadoras, tan solo se refiere a que el servidor esta conectado de "forma comunicativa", sin especificar a que se refiere con esta expresión.

La reivindicación 26 amplía la materia, ya que el dispositivo protector no había sido mencionado en ninguna reivindicación anterior.

La reivindicación 27 menciona una "barrera de fuego", la cual debe especificarse por parte del solicitante, puesto que no queda claro a que se refiere este termino.

La reivindicación 28, nombra un servidor protector conectado en "forma comunicativa" con el servidor de aplicación. Nuevamente se hace la observación acerca de la conexión en forma comunicativa, ya que esta expresión no especifica claramente como es la forma de conexión.

La reivindicación 29 especifica el efecto del uso del sistema: recibir comunicación. Es este caso se debe especificar la estructura de comunicación entre los servidores, no el resultado del proceso de comunicación.

La reivindicación 30 es la misma reivindicación 29 por lo cual debe suprimirse del pliego.

La reivindicación 61 se refiere a una señal de autenticación. Esta señal NO es un elemento de carácter técnico, por lo que no define ninguna característica esencial del sistema de autenticación de la reivindicación 24. Igual situación sucede con la reivindicación 62.

La materia reclamada en las reivindicaciones 37 a 41, ya ha sido presentada en las reivindicaciones anteriores 24 a 29. Los elementos de la reivindicación 24 son un servidor de aplicación y un servidor de autenticación. La reivindicación 28 (que depende de la reivindicación 24) menciona un servidor de protección, es decir que este grupo de reivindicaciones contiene todos los elementos que conforman el sistema de autenticación de la reivindicación 37. De otra parte, la reivindicación 37 y las dependientes de esta, se enfocan en presentar una primera, segunda y tercera clave como elementos característicos del sistema, una clave NO es un elemento técnico que pueda hacer parte de la definición de una invención de producto. Por los motivos anteriores y dado que se esta repitiendo la materia, el pliego no tiene concisión.

Finalmente se tiene que las reivindicaciones 42 y 51, se refieren a una señal legible por computadora y a una señal combinada respectivamente. Estos elementos no pueden considerarse ni producto ni procedimiento, por lo cual la materia reclamada en las reivindicaciones 42 a 59 y 63 a 65, NO se puede considerar objeto de patente.

En conclusión, el pliego reivindicatorio calificado no cumple los requisitos de claridad y concisión, exigidos en el Art. 30 de la Decisión.

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

Los métodos de las reivindicaciones 1 a 23 y 31 a 36, especifican la forma de operación del sistema de autenticación, mediante la aplicación de una secuencia lógica de paso. Tales secuencias se ven representadas en los algoritmos de las figuras 4, 6, 7 y 10 de la solicitud en estudio. En estas figuras se ve claramente que

el objeto de los métodos reclamados corresponde a un una secuencia lógica de etapas (algoritmo) que al ser implementada en un sistema de procesamiento (procesador, computador, servidor, etc.) hace que este realice o ejecute determinada tarea, lo cual es soporte lógico que de acuerdo al literal e) del Art. 15, No puede considerarse patente.

Por otra parte las señales reclamadas en las reivindicaciones 42 y 51, han sido definidas por medio de los datos (información) almacenada en ellas, lo cual se ve con más claridad en las estructuras de las señales mostradas en figuras 5 y 8. De esta manera, un elemento como por ejemplo una señal combinada o una señal legible por computadora, definido por medio de datos tales como la identificación del usuario o datos de la hora, es una forma de presentación de información, lo cual no puede considerarse patente de acuerdo al literal f) del Art. 15 de la Decisión.

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 realizó 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.

No obstante, la solicitud presenta problemas de definición, claridad y concisión, se realizó una búsqueda parcial la cual se complementara una vez se realicen los ajustes a la solicitud.

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

Nº	Documento*	Título	Fecha de publicación
D1	US6609198	LOG-ON SERVICE PROVIDING CREDENTIAL LEVEL CHANGE WITHOUT LOSS OF SESSION CONTINUITY	2003-08-19
D2	US2001/0037469	METHOD AND APPARATUS FOR AUTHENTICATING USERS	2001-10-01

*los documentos mencionados se anexan al expediente

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. Para el examen de novedad únicamente se tuvo en cuenta las características técnicas de la invención, de manera que elementos de carácter no técnico tales como claves, señales, etc. NO fueron considerados ya que de acuerdo a lo expuesto

anteriormente, estos elementos no definen ninguna característica esencial de la invención.

La reivindicación 24 se refiere a un sistema de autenticación dentro de un sistema de computadoras que comprende los siguientes elementos (de carácter técnico):

- 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 valido 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, especifica la 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.

Las reivindicaciones 37 a 41 cubren la misma materia técnica de las reivindicaciones 24 a 30, por lo cual el objeto de este grupo de reivindicaciones tampoco es nuevo.

7. Conclusión:

Los requisitos de patentabilidad de la presente solicitud se encuentran afectados así:

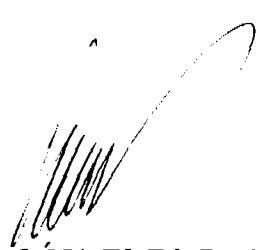
N°	Documento N°	Reivindicaciones afectadas	Requisito que afecta
D1	US6609198	24 a 30, 37 a 41	Novedad
D2	US2001/0037469	24, 25	Novedad

Se recomienda, que tenga en cuenta que el replanteamiento de esos apartes NO podrá implicar una ampliación de la protección que correspondería a la divulgación contenida en la solicitud inicial, de acuerdo a lo que establece el artículo 34 de la Decisión 486.

Si el interesado desea continuar la tramitación, deberá presentar una o más reivindicaciones que definan que defina la materia que se desea proteger, en forma clara, concisa y acorde a lo que establece la ley.

En cumplimiento del artículo 45 de la Decisión 486 de la Comisión de la Comunidad Andina, se le indica que debe dar respuesta dentro del término de sesenta días contados a partir de la fecha de notificación de la presente comunicación. En caso de no dar respuesta al presente requerimiento, o si a pesar de la respuesta subsistieran los impedimentos para la concesión, se denegará la patente.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 5.2, literal e), del capítulo quinto del título primero de la Circular Única N° 10 de 2001.



ALIX CARMENZA CÉSPEDES DE VERGEL
Jefe de División de Nuevas Creaciones

El anterior requerimiento fue notificado por fijación en lista, de fecha

CONCEPTO TÉCNICO No. 2327

EXAMINADOR TÉCNICO
Código No. 202082

MSR