

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO	
RAD: 12-17138- -4	FECHA: 2013-07-25 15:41:00
DEP: 2020 DIRECCION DE NUEVAS CREACIONES	EVE: 378 FASE NACIONAL INCLUIDO CAPITULO I
TRA: 11 PCT-PATENTE DE INVENCION CAPITULOS I Y II	FOLIOS: 5
ACT: 519 PRESENTACION	

DIRECCIÓN DE NUEVAS CREACIONES

2020
Bogotá, D.C.,

Abogado(a)/Señor(a)
MAURICIO PINZON PINZON

Asunto: Radicación: 12-17138- -4
 Trámite: 11
 Evento: 378
 Actuación: 519
 Oficio: 13419
 Folios: 5

Patente de Invención	X			Patente de Modelo de Utilidad	
Vía Nacional					
Vía PCT (Fase Nacional)	X	Capítulo I	X	Capítulo II	
No. Solicitud Internacional	PCT/IB2010/052959				
Fecha de Presentación Internacional	29/06/2010				

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 comunica:

1. Documentos estudiados

Descripción:	Rad. N° 12-017138-00000-0000	01/Febrero/2012
Reivindicaciones:	Rad. N° 12-017138-00000-0000	01/Febrero/2012
Dibujos:	Rad. N° 12-017138-00000-0000	01/Febrero/2012
Prioridad:	IN 1543/MUM/2009	01/Julio/2009

2. Análisis de la Prioridad

Se acepta la reivindicación de prioridad porque ésta solicitud fue presentada dentro del plazo establecido (Art. 9 D 486) y su contenido técnico corresponde con el de la prioridad reivindicada.

3. Objeto de la invención

De acuerdo con lo establecido en el numeral 1.2.2.2 del Capítulo Primero del Título X de la Circular Única para efectos del examen de patentabilidad, se tendrá en cuenta la tasa pagada por el solicitante al momento de comenzar el examen para las reivindicaciones adicionales; esto es que cuando la solicitud contenga más de diez (10) reivindicaciones y no se haya pagado la tasa complementaria, sólo se estudiarán las cubiertas por la tasa pagada. Por lo tanto, se estudiarán las reivindicaciones 1 a 25.

Título de la solicitud: “Método para controlar de manera remota y monitorear los datos producidos en un software de escritorio” (Ver página 1 del radicado N° 12-017138-00000-0000).

El problema planteado en esta solicitud consiste en suministrar un método para proteger el acceso y el uso de datos (archivos, documentos electrónicos, etc.) por personas no autorizadas, a menos que la persona quien realiza dichos datos conceda permisos a un tercero, para el uso y acceso de dichos datos, con el fin de proteger datos confidenciales.

Para resolver este problema técnico, la solicitud en estudio proporciona un método para controlar el uso de datos y prevenir el uso no autorizado de datos que se generan por el software, caracterizado porque usa el sistema de datos ISO.

El objeto de la presente solicitud se relaciona con la Clasificación Internacional de Patentes (CIP): G06F 21/00.

4. De la solicitud de patente

Reivindicaciones (Art 30 D 486, Art 22 PCT)

Las reivindicaciones 3 y 4 no son claras porque los términos “*por lo menos*” y “*uno o más*” son imprecisos, por lo cual no permiten distinguir la invención del estado de la técnica. Se sugiere sustituirlos por un término preciso o un rango concreto.

La reivindicación 1 no es clara ni concisa porque no menciona una serie de pasos llevados a cabo para resolver el problema técnico propuesto; por el contrario, el solicitante se limita a caracterizar su invención por medio del uso de archivos en formato ISO, dejando a un lado las etapas propias de una reivindicación de procedimiento.

Las reivindicaciones 2 a 25 no son claras porque caracterizan la invención por sus resultados a obtener así: “*se pueden usar los datos solamente en la computadora que los ha creado usando el sistema de datos ISO; para usar los datos en otra computadora, el propietario de los datos debe autorizar a un destinatario, usando el mismo sistema de datos ISO en otra computadora*”, “*usar los métodos de intercambio de datos apropiados es decir compartir a través de la subida de datos al servidor en línea o al copiar los datos a cualquier dispositivo de almacenamiento externo*”, “*durante la activación del software, el servidor en línea del vendedor envía dos claves particularmente R1 y R2 al software. La clave R1 se usa para encriptar los datos del propietario para protegerlos el uso no autorizado de estos datos en cualquier otra computadora. Cuando los datos se crean en el software se encriptan con la clave R1 y se almacenan en esta forma encriptada. La clave R2 se usa para proteger los datos que van a ser compartidos con uno o más destinatarios propuestos en su sistema de computadora. Ra y Rb son las claves privadas y públicas del destinatario*”, “*el propietario de los datos puede compartir los datos con el destinatario a través de la subida de datos al servidor en línea, o al transferir los datos a un dispositivo de almacenamiento externo y al compartir este dispositivo con el destinatario*”, “*en caso de que el destinatario todavía no haya registrado la clave R2 del propietario de los datos y los datos a ser compartidos se suban al servidor en línea, los datos primero se desenscriptan usando la clave R1 del propietario de los datos y luego se encriptan con la clave R2 del propietario de los datos. Estos datos se suben al servidor donde se desenscriptan con la clave R2 del propietario de los datos y se encriptan nuevamente con la clave Rb del destinatario. El destinatario descarga estos datos y los usa con su clave Rb*”, “*en caso de que el destinatario todavía*

no haya registrado la clave R2 del propietario de los datos y los datos a ser compartidos se envíen al destinatario a través de un dispositivo de almacenamiento externo, los datos primero se desenscriptan usando la clave R1 del propietario de los datos y luego se encriptan con la clave R2 del propietario de los datos. Estos datos se transfieren al dispositivo de almacenamiento externo y se comparten con el destinatario. El destinatario sube estos datos al servidor en línea y en caso de que el propietario de los datos haya dado permisos suficientes, el servidor desenscripta estos datos con la clave R2 del propietario de los datos y encripta estos datos con la clave Rb del destinatario después de lo cual el destinatario puede descargar y usar estos datos con su clave Rb”, “en caso de que el destinatario haya registrado previamente la clave R2 del propietario de los datos y los datos a ser compartidos se suban al servidor en línea, los datos primero se desenscriptan usando la clave R1 del propietario de los datos y luego se encriptan con la clave R2 del propietario de los datos. Estos datos se suben al servidor, el destinatario descarga estos datos del servidor y desenscripta y usa los datos con la clave R2 del propietario de los datos”, “en caso de que el destinatario haya registrado la clave R2 del propietario de los datos y los datos a ser compartidos a través de un dispositivo de almacenamiento externo, los datos primero se desenscriptan usando la clave R1 del propietario de los datos y luego se encriptan con la clave R2 del propietario de los datos. Estos datos se transfieren al dispositivo de almacenamiento externo y se comparten con el destinatario. El destinatario descarga estos datos del dispositivo de almacenamiento y desenscripta y usa los datos con la clave R2 del propietario de los datos”, “porque el sistema de datos ISO se puede usar para proteger cualquier dato en la computadora/sistema del propietario de los datos”, “porque los datos descargados por el destinatario autorizado y designado se unen por ciertos derechos de acceso expedidos por el propietario de los datos; los datos se pueden usar por el destinatario solamente como por los derechos de acceso establecidos, donde los derechos de acceso establecidos son observar, enmendar, imprimir y guardar”, “porque el destinatario autorizado puede enmendar los datos y enviarlos de nuevo al propietario de los datos si es necesario. Estos datos- enmendados se reconocerán usando un nuevo id de los datos. Los datos se encriptan con la clave Rb y se suben al servidor donde se desenscriptan con la clave Rb y se encriptan nuevamente con la clave R2 del propietario de los datos. El propietario puede descargar estos datos y convertirlos nuevamente a la clave R1 y usarlos”, “porque el destinatario puede enmendar los datos compartidos por el propietario de los datos, si es necesario, y enviar los datos enmendados nuevamente al propietario de los datos ya sea a través de subir los datos al servidor en línea o al transferir los datos a un dispositivo de almacenamiento externo y compartir este dispositivo con el propietario de los datos”, “porque en caso de que el destinatario no haya registrado todavía la clave R2 del propietario de los datos, los datos enmendados a ser compartidos se encriptan con la clave Rb del destinatario y se suben al servidor en línea, donde se desenscriptan con la clave Rb del destinatario y después se encriptan con la clave R2 del propietario de los datos. El propietario de los datos descarga estos datos y los convierte de R2 a su clave R1 y luego los usa”, “en caso de que el destinatario todavía no haya registrado la clave R2 del propietario de los datos y los datos enmendados a ser compartidos se envíen al propietario de los datos a través de un dispositivo de almacenamiento externo, los datos se encriptan usando la clave Rb del destinatario transferida al dispositivo de almacenamiento externo y compartida con el propietario de los datos. El propietario de los datos sube estos datos al servidor en línea y en caso de que el destinatario haya dado suficientes permisos, el servidor desenscripta estos datos con la clave Rb del destinatario y encripta estos datos con la clave R2 del propietario de los datos después de lo cual el propietario de los datos puede descargar estos datos, convertirlos de la clave R2 a la clave R1 y usarlos”, “n caso de que el destinatario haya registrado previamente la clave R2 del propietario de los datos y los datos enmendados a ser compartidos se suban al servidor en línea, el propietario de los datos descarga estos datos y los desenscripta usando su clave R2. Los datos se pueden convertir de la clave R2 a la clave R1 y luego usar”, “en caso de que el destinatario haya registrado previamente la clave R2 del propietario de los datos y comparta los datos

enmendados a través de un dispositivo de almacenamiento externo, el propietario de los datos descarga estos datos del dispositivo de almacenamiento y los descripta usando su clave R2. Los datos se pueden convertir de la clave R2 a la clave R1 y luego usar”, “porque el proceso y almacenamiento de los datos originales y los datos que se reciben para intercambio, se procesan a través de dos subsistemas diferentes y mutuamente exclusivos y están en dos ubicaciones separadas en la misma computadora/sistema”, “porque el propietario de los datos es alertado acerca de la enmienda hecha por el destinatario autorizado en los datos compartidos y puede fusionarlos en los datos originales si es requerido”, “el propietario de los datos puede registrar su clave R2 con otros destinatarios para el propósito de intercambiar datos seguros al enviar al servidor una instrucción para hacerlo de esta manera e ingresar el id del cliente así como también el id del cliente del propietario de los datos. El registro de esta clave se puede revocar en cualquier momento por cualquiera de las partes, al enviar una instrucción al servidor en línea del vendedor acerca del mismo”, “el propietario de los datos puede bloquear los derechos de acceso a los datos compartidos con un destinatario, al instruir al servidor bloquear o suprimir los datos enviados al destinatario”, “porque aún si los datos de la computadora del destinatario, se usa en cualquier otra computadora, no se puede acceder, usar o procesar, debido a la falta de permisos del propietario de los datos”, “porque en caso de que el software sea requerido a ser instalado, se proporciona un fácil método de reinstalación al usuario del software y el servidor envía las claves de encriptado y descriptado nuevamente al software después de la activación. También envía las claves R2 previamente registradas de otro usuario en el software”, “porque en caso que durante la instalación o cada vez que el software se abra, se detecta que el id de la tarjeta madre de la computadora ha cambiado, entonces el software tendrá que ser revalidado con el servidor y también las claves R2 tendrán que ser revalidadas nuevamente por los propietarios de los datos, solamente entonces el intercambio de datos de estos propietarios puede llevarse a cabo”, “el sistema de datos ISO también se puede usar como un módulo de encriptado independiente para asegurar el almacenamiento de datos” lo cual no es permitido ya que equivaldría a definir el problema técnico a resolver y el alcance de la reivindicación incluiría no sólo la solución propuesta por el solicitante, sino todas las alternativas presentes o futuras que lleguen a ese resultado. Se sugiere reemplazarlo por las características esenciales estructurales que contribuyen a la obtención de ese efecto.

Se recuerda al solicitante que las reivindicaciones son las características técnicas esenciales de una invención para las cuales se reclama la protección legal mediante la solicitud de patente. Para el caso de producto, estas deben contener todas las características técnicas de carácter tangible (partes mecánicas, eléctricas, electrónicas y su relación o conexión), las cuales le permitan obtener los usos, resultados o funcionamiento deseado, pueden contener si es necesario referencias de los dibujos para ser más claras, se permite la presencia de signos de referencia entre paréntesis después de la característica mencionada en la reivindicación; para un procedimiento, estas deben divulgar los pasos necesarios para obtener un producto y/o una transformación de un estado inicial, en el caso de invenciones implementadas por computador, los pasos deben estar vinculados con una materia técnica tangible, la cual debe ser específica para el desarrollo de dicho procedimiento, y que resuelva el problema técnico propuesto por la solicitud.

Por lo anterior, el capítulo reivindicatorio de la solicitud en estudio no cumple con el requisito de claridad acuerdo con el artículo 30 de la Decisión 486. En consecuencia, el solicitante deberá presentar un nuevo capítulo reivindicatorio, donde se hayan modificado las objeciones anteriormente citadas; dichas modificaciones no deben ampliar el objeto inicialmente presentado por la presente solicitud.

5. Determinación del Estado de la Técnica

El estado de la técnica se determinó con base en la fecha de presentación de la solicitud de prioridad: julio 01 de 2009 y se encontró el siguiente documento que anticipa el objeto de esta solicitud:

Ítem	Documento	Título	Fecha de Publicación
D1	US 2009/0100060	"Device, system, and method of file-utilization management"	16/Abril/2009

El documento D1¹ divulga un sistema empresarial de administración de derechos digitales (EDRM) que tiene un proceso simplificado de registro, un proceso simplificado de protección de archivos, un proceso simplificado para acceder a un archivo protegido, y/o un proceso simplificado para la gestión y/o actualización de las restricciones de utilización del archivo protegido (Pág. 1, Fl. 10, Párr. 0009).

6. Examen de Patentabilidad (Art 14 D486)

Novedad (Art 16 D486)

Debido a las objeciones realizadas en el numeral 4 del presente oficio, en donde es evidente la falta de claridad y concisión del pliego reivindicatorio, y específicamente la ausencia de una serie de pasos en la reivindicación independiente 1, esta oficina indica que:

La reivindicación 3 consiste en *"El método de conformidad con la reivindicación 1, caracterizado porque comprende:*

seleccionar los datos a ser compartidos e incluir el id del cliente de propietario de los datos;

identificar y autorizar por lo menos a un destinatario con quien los datos van a ser compartidos..." (Ver página 132 del radicado N° 12-017138-00000-0000).

Comparación de las características técnicas esenciales, con las del estado de la técnica:

Características esenciales	D1
Seleccionar los datos a ser compartidos e incluir el id del cliente del propietario de los datos.	Los sistemas EDRM pueden permitir el intercambio seguro de información, permitiendo a los usuarios compartir archivos de forma selectiva con los clientes, socios y/o proveedores, mientras que prohíbe la distribución de los contenidos a personas no autorizadas (Pág. 1, Fl. 10, Párr. 0004). En algunas formas de realización, la vinculación entre la dirección de correo electrónico y el dispositivo informático puede incluir almacenar una etiqueta de identificación del dispositivo de vinculación en asociación con la dirección de correo electrónico vinculado (Pág. 2, FL. 11, Párr. 0025).
Identificar y autorizar por lo menos a un destinatario con quien los datos van a ser compartidos al ingresar el id del cliente del destinatario.	Permitir a un usuario ("el propietario del archivo") definir uno o más permisos de identificación de quién puede y/o quién no puede tener acceso a uno o más archivos "de su propiedad" por el usuario, y/o definir una o varias restricciones de utilización que se aplican selectivamente en uno o más de los usuarios que tienen permiso para acceder al archivo de propiedad ("los usuarios autorizados"). Por ejemplo, el propietario del archivo puede definir que un primer usuario permitido no se puede permitir llevar a cabo una o varias de copiar y pegar el contenido del archivo de propiedad, la modificación de una operación de la pantalla de impresión de una imagen que representa el contenido del archivo de propiedad, la impresión del archivo, la edición del archivo, y/o cualquier otra forma de utilización de la propiedad del archivo, mientras que un segundo usuario permitido puede llevar a cabo una o más de estas operaciones (Pág. 1, Fl. 10, Párr. 0011). La aplicación de servidor (104) y/o la aplicación cliente (140) pueden identificar a un usuario de sistema (100) sobre la base de una dirección de

1 <https://docs.google.com/viewer?url=patentimages.storage.googleapis.com/pdfs/US20090100060.pdf>

	correo electrónico asociada con el usuario (Pág. 5, Fl. 14, Párr. 0085).
Identificar cada conjunto de datos que se comparten por un id de los datos único generado por el sistema del propietario de los datos, donde los permisos de acceso a cada conjunto de datos se asocian con cada id de los datos particulares.	En algunas realizaciones, la solicitud incluye un identificador de archivo para identificar el archivo de aplicación web, en el que el método incluye recuperar el archivo de aplicación web basada en el identificador de archivo (Pág. 1, Fl. 10, Párr. 0018). En algunas formas de realización, el método puede incluir la generación de un enlace incluyendo el identificador de archivo, almacenar el archivo de aplicación web, y almacenar el identificador de archivo en asociación con la información de permisos correspondiente al archivo de aplicación en red, en el que la recepción de la petición incluye la recepción en el enlace (Pág. 1, Fl. 10, Párr. 0019).
Expedir permisos de acceso requeridos al destinatario autorizado para usar los datos.	Comprobar que el usuario está autorizado a acceder a la cuenta de correo electrónico puede incluir el envío a la dirección de correo electrónico un mensaje que incluye primero la información de autenticación y verificación que el usuario está autorizado a acceder a la cuenta de correo electrónico basado en una respuesta recibida como una segunda información de autenticación (Pág. 2, FL. 11, Párr. 0027).

De acuerdo con la tabla anterior, las características esenciales del método de la reivindicación 3 habrían sido divulgadas previamente en el documento D1, por lo tanto, la materia reivindicada no es nueva.

Asimismo, las reivindicaciones 1, 2 y 4 a 25 no mencionan alguna característica que haga nuevo el método reivindicado, debido a que, divulgan las mismas características técnicas de la reclamación 3 o se encuentran redactadas en términos de usos, resultados y/o no incluyen los pasos necesarios para resolver el problema técnico propuesto. Por lo tanto, no se consideran nuevas.

7. Conclusión

Los requisitos de patentabilidad de la presente solicitud están afectados así:

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	US 2009/0100060	1 a 25	Novedad/Nivel Inventivo

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 (60) 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.

Se invita al solicitante se sirva indicar, si así lo considera, su renuncia al término faltante de sesenta (60) días para dar respuesta a este requerimiento y presentarla por escrito.

Finalmente, se le recuerda al solicitante que si como respuesta a este requerimiento llegara a modificar el capítulo reivindicatorio y éste contenga más de diez (10) reivindicaciones, no pagará la tasa de modificación voluntaria pero sí la correspondiente al pago por reivindicación adicional.

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 No. 10 de 2001.



JOSÉ LUIS SALAZAR LÓPEZ
Director de Nuevas Creaciones (c)

El anterior requerimiento fue notificado por fijación en lista, de fecha 2013-07-30

Elaboró: Diego Gonzalez Castillo
Revisó: Angelica Maria Ramirez