39
37

CAVELIER
ABOGADOS

WEB SITE www.cavelier-abogados.com
E-MAIL cavelier@colomsat.net.co

EDIFICIO SISKI
CARRERA 4 No. 72 - 35
BOGOTA 8, COLOMBIA

SUPERINDUSTRIA Y COMERCIO
Radicacion : 00084953 00000001 Folios: 22
Fecha (AMD): 2001-01-09 17:00:49
Tramite : 002 PATENTES D 1 REGISTRO/ 444 REPUESTA
Dependencia: 2020 DIVISION DE NUEVAS CREACIONES

Señora Jefe de la
DIVISION DE NUEVAS CREACIONES
Superintendencia de Industria y Comercio
E. S. D.

Referencia : Expediente No. 00.084.953
Solicitante : **NAGRAVISION S.A.**
Asunto : Solicitud de patente para: **"SISTEMA Y PROCESO CRIPTOGRAFICO CENTRALIZADO DE ELEVADO FLUJO CRIPTOGRAFICO"**
Fecha de la solicitud : Noviembre 8 de 2000

TRAMITE: 002 - EVENTO: 001 - ACTUACION:444

1. Yo, Emilio FERRERO, obrando como apoderado del solicitante en el asunto antes identificado, me refiero al auto número 4005, notificado por estado del 23 de Noviembre de 2000.

2. Mediante el auto número 4005 se puso en conocimiento del solicitante el informe que contiene las observaciones hechas por su Despacho sobre la presente solicitud de patente. Atiendo a las observaciones de la manera siguiente:

2.1. **En la descripción.** Presento junto con este memorial una nueva descripción en la cual se corrigieron errores de transcripción, redacción y/o traducción, de acuerdo con lo requerido por ese Despacho. Le solicito se sirva aceptar este nuevo capítulo descriptivo en sustitución del presentado originalmente.

2.2. **En las reivindicaciones.** Presento junto con este escrito un nuevo pliego reivindicatorio en el cual se han realizado las siguientes modificaciones:

- Se corrigieron errores de trascripción, redacción y/o traducción de las reivindicaciones 3, 5, 8, 12 y 13. Con relación a este punto, se desea aclarar que no se encontró el uso de pronombres en las reivindicaciones 4, 9, 10 y 11 como lo menciona ese Despacho. Por lo tanto, en ese sentido dichas reivindicaciones no han sido modificadas.

- Se modificaron las reivindicaciones 8 a 13 para definir de manera más clara los pasos o etapas del método reivindicado y se modificó el término "método de tratamiento criptográfico" por "método criptográfico" debido a que el tratamiento criptográfico no se encontraba definido como tal en la reivindicación independiente (8).

Le solicito se sirva aceptar este nuevo capítulo reivindicatorio de 13 reivindicaciones en sustitución del presentado originalmente.

Finalmente, solicito a Usted muy comedidamente que si el examinador encuentra alguna discrepancia con respecto a alguna de las anteriores explicaciones, éstas sean informadas junto con el examen de fondo y no constituyan impedimento substancial para el buen desarrollo de esta solicitud de patente.

2.3. **Extracto.** Adjunto a este memorial presento nuevo extracto y nueva tarjeta temática (Formas P-103 y P-104), los cuales están en conformidad con las modificaciones hechas al pliego reivindicatorio.

2.4.**Recibos.** Presento junto con este escrito, el recibo de pago por valor de $68.000.oo pesos por concepto de modificaciones solicitud pendiente.

CAVELIER
ABOGADOS

3. Puesto que se han atendido a cabalidad las observaciones hechas por su Despacho sobre la presente solicitud de patente, atentamente solicito que se continúe su tramitación.

Bogotá, 29 ENE 2001
Señora Jefe,

EMILIO FERRERO
T.P.A. No. 31.929

COLO 12230-801-004-2
ASN-24

SISTEMA Y PROCESO CRIPTOGRAFICO CENTRALIZADO DE ELEVADO FLUJO CRIPTOGRAFICO

La presente invención se refiere a un proceso y sistema criptográfico centralizado, en particular destinado a aplicaciones que necesiten de elevados flujos criptográficos.

En un sistema de servicio distribuido tal como la televisión de pago, el pago por tarjeta bancaria o mediante internet, las informaciones intercambiadas entre un centro de gestión y los módulos usuario, utilizan medios criptográficos para garantizar la autenticidad y el carácter confidencial de los datos.

Según el tipo de aplicación, el número de módulos usuario puede ser elevado y cada uno de estos módulos encauza las informaciones, mediante concentradores, a uno o a los centros de gestión encargados de autenticar y de efectuar las transacciones. Estas operaciones se basan en las comunicaciones encriptadas y necesitan medios criptográficos, por una parte en el lado de los módulos usuario, y por otra parte en el lado del centro de gestión. Se imagina fácilmente que si se quiere tratar un gran número de módulos usuario, los medios criptográficos del lado central deben ser muy potentes mientras que los medios criptográficos del lado usuario, siendo propio a cada usuario, no tienen las mismas necesidades.

Por lo que si un procesador contenido en una tarjeta chip es capaz de tratar estas informaciones al nivel

del módulo usuario, se instala en cambio generalmente ordenadores potentes en el lado del centro de gestión.

Un punto muy importante es el acceso a las claves de encriptación. En el centro de gestión, las operaciones criptográficas son efectuadas en un módulo criptográfico especializado, para lo cual se debe poner una atención particular en lo que se refiere a la seguridad. Estos están compuestos entre otros, de un procesador de alta capacidad, dedicado a las operaciones criptográficas, y una memoria que contiene las claves. Por razones de seguridad, estos módulos están bien situados en un recinto protegido tal como una cámara o local cerrado, bien encapsulados en una caja cuya abertura por cualquier método provoca el borrado de las informaciones sensibles.

A pesar de que estas disposiciones presentan innegables cualidades, estos módulos son débiles en cuanto a su estructura electrónica y pueden ser vulnerables a un operador malintencionado. En efecto, el empleado poseedor de la llave que le permite abrir el local donde se sitúan los módulos criptográficos puede fácilmente acceder a la memoria donde son almacenadas las claves criptográficas. Una intromisión así puede ser catastrófica para la seguridad del sistema y la credibilidad del proveedor de servicio.

Además estos módulos criptográficos, a pesar de tener una elevada capacidad de tratamiento, no presentan flexibilidad cuando se requieren capacidades superiores. Un

aumento de la potencia del 10% por ejemplo implica el desdoblamiento del módulo criptográfico, lo que hace aumentar la capacidad al 100%. Otro aspecto concierne la actualización de estos módulos que es difícil para una tarjeta desarrollada especialmente con este fin.

Es conocido el hecho de utilizar más de una tarjeta chip para las operaciones de desencriptación en el módulo de abonado y esta configuración está descrita en el documento WO 96/07267 así como la publicación EBU Review Technical No. 266 "Functional Model of a Conditional Access System". Sin embargo, la presencia de estas tarjetas múltiples situadas en el lado del receptor está dictada pro el hecho que se necesite desencriptar varias fuentes utilizando claves diferentes, es decir, funciones criptográficas diferentes. La presencia de estas tarjetas no permite resolver el problema del tratamiento de un flujo importante de datos sino únicamente asegurar la contabilidad con diversos estándares.

El problema que se propone resolver la presente invención es proporcionar un módulo criptográfico que presenta una alta seguridad contra la intrusión tanto al nivel físico como del software, una gran flexibilidad en función de las necesidades en los flujos criptográficos y que permite una actualización fácil.

Este objetivo es plenamente alcanzado por un sistema criptográfico centralizado que comprende un módulo de control y al menos un módulo criptográfico, caracterizado

porque cada módulo criptográfico está compuesto de uno o varios módulos interfase sobre el cual se halla una o varias unidades de seguridad monolítica.

Se entiende por unidad de seguridad monolítica una unidad que incluye todos los elementos necesarios para las operaciones criptográficas y que están reunidos en un soporte único con el fin de establecer la seguridad. Estas están generalmente compuestas de un solo chip electrónico, chip que dispone de una protección antiintrusión mecánica o electrónica. Otras estructuras compuestas de, por ejemplo, dos chips electrónicos, están igualmente incluidas en la denominación "monolítica" ya que están íntimamente unidas y son suministradas por los distribuidores como un solo elemento.

Según la invención, el módulo criptográfico comprende un primer módulo de control encargado de llevar las entradas/salidas de informaciones que deben ser encriptadas. Éste permite determinar el flujo criptográfico deseable y conoce el flujo criptográfico disponible. Este módulo de control puede ser o material o software. Para efectuar el tratamiento de las informaciones, dispone de uno o varios módulos interfase sobre el que se encuentran las unidades de seguridad monolítica. Cada una de estas unidades comprende una unidad de cálculo criptográfico, una memoria que contiene al menos una parte de las claves de encriptación y los medios para comunicar con el módulo interfase. Las claves se encuentran descifradas únicamente en las unidades de

seguridad que son, como se ha indicado anteriormente, de un alto nivel de seguridad. Este nivel se alcanza gracias al hecho de que éstas son de un solo circuito proyectado y homologado con este fin. Sus estructuras no les permiten alcanzar capacidades de tratamiento elevadas y es por esta razón que el flujo criptográfico está asegurado para la utilización de un gran número de las unidades. Cuanto más aumenta el flujo requeridc por el sistema criptográfico mayor es el número de las unidades en funcionamiento.

Dicha configuración permite asegurar una gran flexibilidad en cuanto a los flujos criptográficos del conjunto mediante la adición de unidades de seguridad en función de las necesidades. Dicha configuración permite seguir la demanda añadiendo las unidades de seguridad necesarias.

Según una forma de la invención, las unidades de seguridad monolítica están montadas en los módulos interfase de manera amovible. Eso permite una actualización más fácil de estos últimos, evolucionando la tecnología rápidamente. Otra ventaja de esta solución es su costo, ya que las unidades de seguridad son fabricadas en gran cantidad, beneficiándose así de un precio atractivo.

Según una forma de la invención, las unidades de seguridad son tarjetas chip que responden a las normas ISO 7816.

La presente invención se refiere igualmente a un método de tratamiento criptográfico centralizado de informaciones que consiste en transmitir las informaciones que deben ser encriptadas a un módulo criptográfico, donde dicho módulo comprende uno o varios módulos interfase y el cual transmite, por medio de dichos módulos interface, dichas informaciones a una o varias unidades de seguridad monolítica encargada de las operaciones criptográficas según el flujo de informaciones.

Según este método, el número de unidades de seguridad en servicio depende del flujo de informaciones solicitada al módulo criptográfico. En efecto, dado que cada unidad no tiene la prestación suficiente para tratar un gran número de informaciones criptográficas en un tiempo corto, se llama a varias unidades de seguridad. El módulo de control y el módulo de interfase autorizan la puesta en paralelo de los recursos de las unidades de seguridad.

Una de las funciones del módulo de interfase es la gestión de los recursos disponibles posteriormente. El módulo de interfase efectúa en una fase de inicialización, el inventario de las unidades de seguridad que le son asociadas así como sus características. Este fichero de recursos servirá para encauzar las solicitudes según las características de estas unidades.

Según una modalidad de la invención, el método consiste en hacer ejecutar las mismas operaciones

criptográficas por varias unidades de seguridad y comparar los diferentes resultados. Si los resultados difieren, el módulo de control envía un mensaje de error a la consola. Esta última puede reaccionar de diferentes maneras, por ejemplo establecer cual de las unidades de seguridad es responsable del error ya sea cuando se utiliza una unidad de seguridad de referencia, bien varias unidades de seguridad, detectando así aquella que reenvía un resultado diferente.

El resultado de este test será notificado a la lista de recursos para que la o las unidades defectuosas no vuelvan a ser utilizadas.

En la hipótesis de que el error no venga de una unidad de seguridad sino que concierne a todas las unidades de un mismo módulo interfase, las operaciones criptográficas paralelas son ejecutadas por dos unidades de seguridad situadas en dos módulos interfase diferentes. En efecto, ciertos parámetros son almacenados en el módulo interfase y su modificación puede acarrear la disfunción de todas las unidades de seguridad.

Con el fin de asegurar el buen funcionamiento de estos módulos diferentes, es posible hacer ejecutar operaciones de test sobre las unidades de seguridad no utilizadas. Estos test pueden ser efectuados en base a datos de referencia cuyo resultado es previamente conocido, o efectuarse testando en paralelo varios módulos con datos generados aleatoriamente y comparando los resultados.

La invención será mejor comprendida gracias a la descripción detallada que sigue a la continuación y que se refiere a los dibujos anexos que son dados a modo de ejemplo en modo alguno limitativo, en los cuales:

- La figura 1 representa un sistema centralizado criptográfico según el estado actual de la técnica;
- La figura 2 representa un sistema criptográfico según la invención;

En la figura 1 están representados esquemáticamente los diferentes bloques del conjunto responsable del encriptado en un centro de gestión. Los datos a ser encriptados se encuentran en el bus que transmiten las diferentes informaciones necesarias para el funcionamiento del centro de gestión se hallan las informaciones que deben ser encriptadas. Cuando una operación así es solicitada por el centro de gestión, se llama al sistema criptográfico especializado representado aquí por el bloque módulo de control CM y el bloque módulo criptográfico EM. El módulo de control CM tiene como misión filtrar los accesos al módulo criptográfico EM, es decir que ofrece una protección para los ataques provenientes del exterior a través del bus de comunicación. Dicho módulo de control no está concebido para resistir a un ataque local, ya sea físico o "informático", por el operador por ejemplo.

Dicho módulo de control CM, después de haber filtrado las informaciones, las transmite al módulo criptográfico EM para su tratamiento. Como se ha indicado más arriba, dicho módulo comprende medios potentes para ejecutar en un tiempo muy corto las operaciones criptográficas con el fin de satisfacer los elevados flujos del bus central. Para ello dispone de las claves descifradas en su memoria. Para nuestro ejemplo, dicho módulo está ubicado en un recinto protegido físicamente para evitar que un tercero pueda extraer las claves o modificar el soporte lógico en su beneficio.

En la figura 2 está representada la arquitectura del sistema según la invención. Volvemos a encontrar el módulo de control CM que funciona como filtro de soporte lógico para las intrusiones externas. Como se ha indicado en la figura 2, dicho módulo está conectado a varios módulo interfase IM. Dichos módulos poseen una protección de soporte lógico, es decir que un cierto número de operaciones (la lectura por ejemplo), son completamente imposibles. Dichos módulos no están sin embargo protegidos físicamente, dejándose esta función a las unidades de seguridad PIM. Cada módulo interfase IM comprende un cierto número de estas unidades PIM con el fin de aumentar los flujos criptográficos.

Otra tarea de este módulo CM es la de dirigir las solicitudes que provienen del bus central hacia las unidades de seguridad. Cuando la operación deseada está terminada

(encriptación por ejemplo), el resultado es transmitido al módulo CM que informa a la entidad que ha requerido esta operación. Para asegurar la distribución de las solicitudes, el módulo CM dispone de una lista de los recursos disponibles. Cuando se detecta un error, la unidad responsable es desactivada en el panel de recursos.

No es necesario que todas las unidades de seguridad sean del mismo tipo. Puede que algunas dispongan de unidad de cálculo criptográfico basado en un algoritmo diferente a las otras unidades. Para nuestro ejemplo, ciertas unidades disponen por ejemplo de una unidad de tipo RSA, otras de una unidad de tipo DES o IDEA.

Estas informaciones están contenidas en la lista de recursos almacenada en el módulo CM. Este módulo encauza las solicitudes en función de las disponibilidades y en función de las capacidades de las unidades de seguridad.

Según un variante de la invención, los módulos de interfase son tarjetas de tipo PCI y las unidades de seguridad son tarjetas chip de tipo ISO 7816.

A pesar de que la presente invención se refiere en primer lugar a la encriptación de datos, la arquitectura descrita más arriba es igualmente aplicable para la desencriptación de un flujo de datos. En efecto, es posible que en el momento de la compra de una emisión por ejemplo, los usuarios accedan en gran número al centro de gestión y

generen un flujo importante que debe ser desencriptado. Las unidades de seguridad scn por lo tanto solicitadas para operaciones de desencriptación de datos.

REIVINDICACIONES

1. Sistema criptográfico centralizado que comprende un módulo de control (CM) y al menos un módulo criptográfico (EM), caracterizado porque cada módulo criptográfico está compuesto de uno o varios módulos interfase (IM) sobre el cual está conectada una o varias unidades de seguridad monolítica (PIM).

2. Sistema según la reivindicación 1, caracterizado porque la unidad de seguridad comprende al menos una unidad de cálculo para las funciones criptográficas, una memoria que contiene claves criptográficas y medios de comunicación con el módulo interfase.

3. Sistema según las reivindicaciones 1 ó 2, caracterizado porque la unidad de seguridad se encuentra montado de una manera amovible en el módulo interfase.

4. Sistema según las reivindicaciones 1 a 3, caracterizado porque la unidad de seguridad monolítica es una tarjeta chip.

5. Sistema según la reivindicación 4, caracterizado porque dicha tarjeta chip responde a las normas ISO 7816.

6. Sistema según una de las reivindicaciones precedentes, caracterizado porque las unidades de seguridad

monolítica (PIM) tienen unidades de cálculo criptográfico de tipo diferente tales como RSA, DES, T-DES o IDEA.

7. Sistema según una de las reivindicaciones precedentes, caracterizado porque el módulo de control (CM) comprende una lista de recursos de las unidades monolíticas que comprende el número disponible, su estado, su versión y su capacidad criptográfica.

8. Método criptográfico centralizado de informaciones que consiste en:

- transmitir informaciones que deben ser encriptadas o desencriptadas a un módulo de control (CM), que comprende uno o varios módulos interfase
- transmitiendo dicha información a dichos módulos interfase, este módulo comprendiendo una pluralidad de unidades de seguridad monolíticas, enrutando dicha información unidades de seguridad monolítica encargadas de las operaciones criptográficas según el flujo de informaciones.

9. Método criptográfico según la reivindicación 8, caracterizado porque consiste en:

- enrutar a varias unidades de seguridad la misma información a ser procesadas

- comparar la información devuelta por las unidades de seguridad, e

- informar a una entidad exterior si los valores difieren.

10. Método criptográfico según la reivindicación 9, caracterizado porque consiste en:

- enrutar la información a ser procesada a unidades de seguridad situadas en módulos interfase diferentes.

11. Método criptográfico según la reivindicación 8, caracterizado porque consiste en:

- efectuar operaciones de prueba en una o varias de las unidades de seguridad no utilizadas en el momento y

- comparar el resultado con un resultado de referencia.

12. Método criptográfico según la reivindicación 8, caracterizado porque consiste en:

- efectuar operaciones sobre al menos tres unidades de seguridad no utilizadas actualmente, y
- comparar los resultados para determinar si las unidades funcionan.

13. Método criptográfico según las reivindicaciones 8 a 12, caracterizado porque consiste en:

56
54

- administrar las unicades de seguridad gracias a una lista de recursos situada en el módulo de control (CM), comprendiendo dicha lista el número de unidades disponibles, su estado, su versión y su capacidad criptográfica.

RESUMEN

En un sistema de servicios distribuidos tal como la televisión de pago, las informaciones intercambiadas entre un centro de gestión y módulos usuarios utilizan medios criptográficos para garantizar la autenticidad y el carácter confidencial de los datos. Las necesidades de tratamiento criptográfico en el centro de gestión son importantes y por eso se propone un sistema criptográfico que une modularidad y seguridad para la utilización, para las operaciones criptográficas, de unidades de seguridad monolítica tales como tarjetas chip.

(Figura 2)

COLO 12230-801-004-2

ASN/id-25

Industria y Comercio

SUPERINTENDENCIA

SUPERINDUSTRIA Y COMERCIO
Radicacion : 00084953 00000001 Folios: 22
Fecha (AMD): 2001-01-09 17:00:49
Tramite : 002 PATENTES D 1 REGISTRO/ 444 PETICION
Dependencia: 2020 DIVISION DE NUEVAS CREACIONES

NIT : 800176089-2

RECIBO OFICIAL DE CAJA : 547
FECHA : ENERO 5 DE 2001

C O N S I G N A C I O N

DEPOSITANTE	TIPO PAGO	BANCO	SUCURSAL	CUENTA	No. PAGO	Vr. PAGO
CAVELIER ABOGADOS	CONSIGNACION	BANCO POPULAR	BOGOTA	050-00110-6	1798648	1,152,000.00

C O N C E P T O

CANT.	RENTISTICO	CONCEPTO	TOTAL CONCEPTO
1	50005-01-03 CAMBIO DE MODALIDAD Y MODIFICA	12 MARCAS Y LEMAS COMERCIALES	68,000.00
		TOTAL : $	68,000.00

SON: SESENTA Y OCHO MIL PESOS

RESPONSABLE : _____

RECIBO DE CAJA APLICADO AL EXPEDIENTE No._____

Carrera 13 No 27-00 Pisos 5, 7 y 10
Conmutador 382 0840
Fax 350 5220
e-mail info@sic gov co
www sic gov co
Bogotá, D C ,Colombia

57

2do. EXAMEN DE FORMA PATENTE DE INVENCION

Folio 61

Radicación no 00-84953

Concepto Técnico no 366
Clasificación Internacional de Patentes: H04N7/16//H04L9/32

Practicado el examen de acuerdo a lo establecido en el Art. 38 de la Decisión 486 se determinó que esta solicitud de **Patente de Invención:**

SI [✔] NO [ ] Contiene un resumen de la invención (Art.26-e).

SI [✔] NO [ ] Contiene el título o nombre de la invención (Art.27-d).

SI [✔] NO [ ] Contiene la descripción de la invención (Art.26-b).

SI [✔] NO [ ] NO ES APLICABLE [ ] Contiene los dibujos necesarios para comprender la invención (Art.26-d)

SI [✔] NO [ ] Contiene una o más reivindicaciones. (Art.26-c).

SI [ ] NO [ ] NO ES APLICABLE [✔] Han sido desarrollados los productos y/o procedimientos a partir de recursos genéticos o de sus productos derivados de los que cualquiera de los Países Miembros es país de origen. (Art. 26- h).

SI [ ] NO [ ] NO ES APLICABLE [✔]Los productos y/o procedimientos han sido obtenidos o desarrollados a partir de los conocimientos tradicionales de las comunidades indígenas, afroamericanas, o locales de los países miembros, de acuerdo a lo establecido en la Decisión 391 y sus modificaciones y reglamentaciones vigentes.(Art.26-i).

SI [ ] NO [✔] La invención se refiere a un producto relativo a un material biológico. (Art.26-J).

SI [✔] NO [ ] La prioridad coincide con la materia reivindicada.

SI [✔] NO [ ] CUMPLE LOS REQUISITOS TÉCNICOS

OBSERVACIONES Y OTROS: SI [✔] NO [ ] ver hoja(s) anexa(s)

EXAMINADOR TÉCNICO
202049

Bogotá D. C., 10 de Febrero de 2003

Industria y Comercio
SUPERINTENDENCIA

58

Folio 62

Radicación no 00-84953
Concepto Técnico no 366

OBSERVACIONES:

1. Se presenta nuevo capítulo descriptivo en los folios 42 a 52.
2. Se presenta nuevo capítulo reivindicatorio y resúmen en los folios 53 a 57.
3. Se presenta nueva tarjeta para archivo temático y nuevo extracto para publicación.

EXAMINADOR TÉCNICO
202049

Bogotá D. C., 10 de Febrero de 2003

Industria y Comercio
SUPERINTENDENCIA

89

Folio: 83

2020
Bogotá DC

Doctora
EMILIO FERRERO
Apoderado

REFERENCIA:	Radicación No.	00-84953
	Trámite	002
	Evento	001
	Actuación	416
	Oficio No.	326
	Folios	001

Teniendo en cuenta que la solicitud de privilegio de patente que se tramita bajo el expediente indicado en la referencia, reúne los requisitos de forma establecidos en los artículos 26 y 27 de la Decisión 486 de la Comisión de la Comunidad Andina, y en las demás disposiciones vigentes sobre la materia, se envía el extracto de la solicitud a la Oficina de Comunicaciones para efecto de su publicación en la Gaceta de Propiedad Industrial, conforme lo establece el artículo 40 de la misma Decisión.

Cúmplase
Dado en Bogotá DC, a los 14 FEB. 2003

ALIX CARMENZA CÉSPEDES DE VERGEL
Jefe de la División de Nuevas Creaciones

202049

Carrera 13 No. 27-00 Piso 5 y 10
Conmutador: 334 12 21-2-3-4
Fax: 281 31 25 e-mail: info@sic.gov.co
Santa Fe de Bogota D.C. - Colombia

64
60

Industria y Comercio
SUPERINTENDENCIA

DIVISION DE NUEVAS CREACIONES

RADICACIÓN EXPEDIENTE No 00-084953

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

FUE PUBLICADO EN LA GACETA DE PROPIEDAD INDUSTRIAL No **530**, DE

FECHA **31** DE **JULIO DE 2003**, EL TERMINO HABIL SEÑALADO POR LA LEY

EXPIRA EL **28** DE **OCTUBRE** DE **2003**

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 _ _ _____

Bogotá D C , ABRIL DE 2005