

Industria y Comercio
S U P E R I N T E N D E N C I A

DELEGATURA DE PROPIEDAD INDUSTRIAL

División de Nuevas Creaciones

SOLICITUD
PATENTE DE INVENCION

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 12-171852- -00000-0000

Fecha: 2012-10-01 16:10:46 Dep. 2020 DIR.NUEVASCR
Tra. 11 PATENTEIYII Eve: 378 FASENACIONALI
Act. 411 PRESENTACION Folios: 26 25

21. **EXPEDIENTE No.** _____

54. **TÍTULO** _____
PROCEDIMIENTO Y DISPOSITIVO DE AUTENTICACION

51. **CLASIFICACIÓN INTERNACIONAL** _____
H04W 12/04

71. **SOLICITANTE** _____
EKO INDIA FINANCIAL SERVICES PVT. CO

DOMICILIO _____
NUEVA DELHI, INDIA

74. **APODERADO** _____
LUIS FELIPE CASTILLO GIBSON

22. **BOGOTÁ, D.C.,** _____
01 OCT. 2012



No. 12-171852- -00000-0000

Fecha: 2012-10-01 16:10:46 Dep. 2020 DIR.NUEVASCR
Tra. 11 PATENTEIYII Eve: 378 FASENACIONALI
Act. 411 PRESENTACION Folios: 26 25



DIRECCIÓN DE NUEVAS CREACIONES
SOLICITUD FASE NACIONAL - PCT

1	TIPO SE SOLICITUD	☒ Patente de invención ☒ Capítulo I	☐ Patente de Modelo de Utilidad ☐ Capítulo II
2	DATOS SOLICITUD INTERNACIONAL PCT (86)		
Solicitud Internacional No.		PCT/ IN2011/000128	Fecha 01.03.2011
Publicación Internacional No.		WO 2011/108004 A1	Fecha 09.09.2011
3	TÍTULO DE LA INVENCIÓN (200 caracteres o espacios máximos)		
PROCEDIMIENTO Y DISPOSITIVO DE AUTENTICACIÓN			
4	CLASIFICACIÓN INTERNACIONAL (CIP)		
H04W 12/04			
5	SOLICITANTE (S) ☐ Esta persona también es inventor. Para datos adicionales utilizar hoja de información complementaria		
EKO INDIA FINANCIAL SERVICES PVT. LTD.		IDENTIFICACIÓN	TIPO
6	DATOS DEL SOLICITANTE		
DIRECCIÓN		547 Mandakini Enclave, Alaknanda	No. TELÉFONO
CIUDAD		Nueva Delhi, India	CORREO ELECTRÓNICO
PAIS			NACIONALIDAD O LUGAR DE CONSTITUCIÓN
7	INVENTOR (ES) Para datos adicionales utilizar hoja de información complementaria		
APELLIDOS		NOMBRES	NACIONALIDAD
1	Abhinav SINHA - Abhishek SINHA - Anupam VARGHESE - Prasad NALDURAG -		IN
2	Raghav BHASKAR - Saurabh PANJWANI		IN
3			IN
4			IN
5			IN
DIRECCIÓN DE CORREO ELECTRÓNICO:			
8	DATOS INVENTOR (ES)		
PAÍS RESIDENCIA	DEPARTAMENTO/ESTADO	CIUDAD	DIRECCIÓN
1 IN	Gurgaon	South City I	601 Tower 7, The Palm
2 IN	Gurgaon	South City I	600 Tower 7, The Palm
3 IN		Nueva Delhi	41A Mig Flats DDA, Sheikh Sarai Phase I,
4 IN	Bangalore	Vasanth Nagar	Flat 812 Embassy Habitat, Palace Road,
5 IN	Bangalore	Jalahalli East	1081, Tower Albany, Prestige Welling-ton Park, I.A.F. Main Road
6 IN	Bangalore	Benson Town	S-3, Sree Vadrevu, #24 Benson A Cross
OTRO(S) SOLICITANTE(S) Y/O (OTRO(S)) INVENTOR(ES)			
☐ Los demás solicitantes y/o (demás) inventores se indican en una hoja a continuación			
9	☐ REPRESENTANTE LEGAL ☒ APODERADO		
LUIS FELIPE CASTILLO GIBSONE		IDENTIFICACION C.C. 79.397.879 de TP 68.995 del Bogotá C.S.J.	
DIRECCIÓN	Carrera 13 No. 37-43 Piso 12	No. TELÉFONO	285 7460
CIUDAD	Bogotá, D.C.	CORREO ELECTRÓNICO	info@castillograu.com
PAIS	Colombia	No. RADICACIÓN O PORTOCOLO DE PODER GENERAL	

2

10	DECLARACIONES DE PRIORIDAD ☒ SI ☐ NO			
(33)PAIS DE ORIGEN		CÓDIGO PAIS	(31) NUMERO	(32) FECHA (AAAA/MM/DD)
1	INDIA	IN		
2			451/DEL/2010	02.03.2010
3				
11	DECLARACIÓN SOBRE USO DE RECURSOS GENÉTICOS O BIOLÓGICOS			
Declaro que el objeto de la presente solicitud de patente fue obtenido a partir de recursos genéticos o biológicos de los que cualquiera de los países miembros de la Comunidad Andina es país de origen,				
☐ SI ☒ NO				
Nota: En caso afirmativo deberá anexar copia del contrato de acceso de recursos genéticos o productos derivados, o certificado o número de registro, expedido por la Autoridad competente,				
12	DECLARACION SOBRE USO DE CONOCIMIENTOS TRADICIONALES			
Declaro que el objeto de la presente solicitud de patente fue obtenido a partir de conocimientos tradicional de comunidades indígenas, afroamericanas o locales de países miembros de la Comunidad Andina.				
☐ SI ☒ NO				
Nota: En caso afirmativo deberá anexar la licencia o autorización de uso de conocimiento tradicional, o certificado o número de registro expedido por la Autoridad competente.				
13	REDUCCIÓN DE TASAS			
Declaro que carezco de medios económicos para presentar la solicitud de la patente.				
☐ SI ☒ NO				
Nota: En caso de ser persona natural y carecer de medios económicos, y por lo tanto, aplique la reducción de tasas a que se refiere la resolución vigente en tarifas, debe firmar la presente solicitud bajo la gravedad de juramento.				
Micro, pequeñas y medianas empresas ☐				
Universidades públicas o privadas ☐				
Entidades sin ánimo de lucro ☐				
Debe aportar los documentos que se indican en el numeral 17 de anexos				
14	AUTORIZACION DE NOTIFICACIÓN EN LÍNEA ☐ SI ☒ NO			
Manifiesto que he leído y entendido perfectamente los términos y condiciones de uso de medios electrónicos para las notificaciones en línea a través de internet de los actos administrativos proferidos por la Superintendencia de Industria y Comercio que deben ser notificados personalmente y, en consecuencia, autorizo el servicio de notificación a través de internet.				
15	COMPROBANTE DE PAGO O PAGO ELECTRÓNICO	No.	Fecha.	
16	FIRMA DEL SOLICITANTE, DEL APODERADO O DEL REPRESENTANTE LEGAL			
Junto a cada firma, indicar el nombre del firmante y su calidad (si tal calidad no es obvia al leer el petitorio)				
LUIS FELIPE CASTILLO GIBSONE				
17	ANEXOS			
Documentación Técnica		Documentación Jurídica		
Solicitud Internacional en Castellano				
1	☒ Descripción	No. De folios:	9	☐ Poderes, si fuera el caso.
2	☒ Reivindicaciones	No. Reivindicaciones:	10	☐ Documento que legalmente pruebe la cesión del inventor al solicitante o a su causante
3	☐ Dibujos y/o figuras	No. Folios:	11	☐ Copia del contrato de acceso de recursos genéticos o productos derivados, o certificado número de registro, si fuera al caso
4	☒ Resumen		12	☐ Copia de la licencia o autorización de conocimientos Tradicionales, o certificado o número de registro, si fuera el caso
5	☐ Certificado de depósito de material biológico si fuera el caso		13	☐ Reducción de tasas
6	☐ Listado de secuencias de nucleótidos y/o aminoácidos en forma digital si fuera el caso		Micro, pequeñas o medianas empresas	
7	☒ Arte final 12 x 12		☐ Copia simple de la declaración de renta del año inmediatamente anterior, o en su defecto prueba documental idónea	
8	☐ Anexo formato digital		☐ Documento de constancia de cumplimiento con lo establecido en la ley 905 de 2004	
			Universidades públicas o privadas	
			☐ Copia acto de reconocimiento institucional emitido por el Ministerio de Educación	
			Entidades sin animo de lucro	
			☐ Copia de regido vigente en Cámara de comercio	
			☐ Hoja de información complementaria	
			☐ Otros, especificar	
			16	☒ Comprobante de pago de la tasa de presentación de la solicitud
			17	☐ Comprobante de pago por reivindicación de prioridad
			18	☐ Comprobante de pago de la tasa de concepto de excedente de palabras en la publicación
			19	☐ Comprobante de pago por reivindicación adicional a 10

17.02.43

PROCEDIMIENTO Y DISPOSITIVO DE AUTENTICACIÓN

APLICACIÓN DEL INVENTO

- 5 **[001]** El presente invento comprende un método de autenticación. Específicamente, la presente invención proporciona un método y un dispositivo que, utilizando una larga clave criptográfica, implementan un método de protección conocido como «número de identificación personal (PIN)» para la autenticación del usuario.

10 **Antecedentes del invento**

- 15 **[002]** Los avances en los campos del comercio y las comunicaciones web y móvil han tornado a la autenticación segura en uno de los más importantes requisitos para cualquier organización cuyas operaciones están basadas tanto en el comercio electrónico como en el móvil. Son diversas las situaciones que requieren la autenticación de un usuario, especialmente en casos de transacciones financieras, y se prevé que tales situaciones aumenten con el paso del tiempo.

- 20 **[003]** El incremento de la entrada al mercado de dispositivos móviles de mano provoca el aumento de las aplicaciones diseñadas para los mismos. Es esencial, al usar algunas de tales aplicaciones móviles, que el usuario disponga de la habilidad de autenticarse a sí mismo ante otros o ante proveedores de servicios en la red de telefonía móvil. Una de tales aplicaciones es el servicio bancario basado en telefonía móvil, por medio del cual los usuarios mantienen cuentas bancarias con una autoridad central (estando ambos conectados a través de una red de telefonía móvil) y transfieren fondos de su cuenta a la de otro usuario utilizando un protocolo de mensajería telefónica. Siempre que la autoridad bancaria recibe una solicitud para tal tipo de transacción de parte de un usuario, primero debe autenticarlo y sólo entonces permitir que la misma se lleve a cabo.

- 30 **[004]** Los sistemas bancarios basados en telefonía móvil están volviéndose populares en muchas partes del mundo, especialmente en los países en desarrollo. La implementación de protocolos de autenticación en los teléfonos móviles en el mundo en desarrollo es un desafío, ya que un gran número de los mismo tienen capacidades de almacenamiento de información y computación bajas y por lo tanto no permiten la implementación de algoritmos criptográficos robustos que uno querría utilizar para la autenticación segura de un usuario. La situación se ve agravada por el hecho de que los fabricantes de teléfonos móviles están aumentando su inversión en teléfonos de gama baja debido a su creciente demanda en zonas rurales, pero sin esforzarse paralelamente en equiparlos con características de seguridad. De hecho, varias de las actuales soluciones para la implementación de una comunicación segura a través de redes de telefonía móvil

4

(por ejemplo, las de telefonía basada en GSM) han demostrado ser fácilmente susceptibles a ataques.

5 [005] Una solución para la autenticación al usar servicios bancarios basados en la telefonía móvil, consignada en papel, se propone en un artículo titulado «Servicios Bancarios Seguros, Sin Sucursales » por Ashlesh Sharma y Lakshmi Subramanian y Dennis Shasha de la Universidad de Nueva York, publicado en NSDR [Por favor, proporcione el Formulario completo] 2009. La solución propuesta se basa en la transmisión de nonces aleatorios frescos y de un identificador basado en la voz por transacción. Por lo tanto, la solución propuesta no es fácil de usar y requiere el soporte de software adicional.

15 [006] En consecuencia, se requiere un dispositivo y método de autenticación fuerte, fiable y resistente a las violaciones de seguridad cuyo uso, a la vez, sea fácil para una gran variedad de usuarios procedentes de diversos medios socioculturales. También es necesario un dispositivo y método de autenticación que pueda implementarse en teléfonos de gama baja sin requerir la instalación de ningún software criptográfico y sin modificar los protocolos de comunicación utilizados para mensajería móvil.

20

Reseña del invento

25 [007] Este invento proporciona un método para la autenticación de un usuario de un dispositivo móvil por una autoridad de verificación, utilizando por lo menos un número de identificación personal (PIN) y al menos una clave criptográfica, siendo los mismos conocidos sólo por el usuario y la autoridad de verificación. La clave criptográfica comprende al menos una clave de sesión. El método comprende por lo menos los siguientes pasos: a. la codificación del PIN por parte del usuario mediante al menos una clave de sesión; b. la transferencia del PIN codificado por parte del usuario a una dirección predefinida de la autoridad de verificación mediante el dispositivo móvil; c. la decodificación del PIN por la autoridad de verificación utilizando la clave criptográfica; y d. la autenticación del usuario por la autoridad de verificación si el PIN decodificado coincide con uno almacenado correspondiente al usuario. En un modelo factible el dispositivo móvil es un teléfono móvil mientras que en otro es una computadora portátil.

35

40 [008] En un modelo factible el PIN comprende una secuencia de un número de caracteres predefinido y sólo conocida por el usuario y la autoridad de verificación. La etapa de codificación del PIN mediante una clave criptográfica comprende el reemplazo de cada carácter del mismo por un carácter correspondiente a al menos una clave de sesión. En un modelo factible la clave criptográfica comprende una secuencia de dígitos, donde cada dígito es seleccionado aleatoriamente del con-

40

junto de números {0,1,..., 9} usando un generador de números aleatorios seguro, estando la clave criptográfica dividida en una o más claves de sesión de 10 dígitos.

5 **[009]** Se le proporciona al usuario una clave criptográfica que comprende una pluralidad de claves de sesión, siendo cada una usada para autenticar al usuario sólo una vez. En un modelo factible la clave criptográfica es provista en forma de un folleto de papel. Mientras en otro modelo factible la clave criptográfica comprende una secuencia de alfabetos, donde cada alfabeto es seleccionado aleatoriamente a partir de un alfabeto predefinido mediante un generador de alfabetos aleatorios seguro, estando la clave criptográfica dividida en una o más claves de sesión que comprenden un número predefinido de alfabetos, siendo presentados al usuario uno o más códigos de transformación en una pluralidad de estilos de presentación.

15 **[0010]** En un modelo factible una clave de sesión usada para codificar el PIN una vez es extraída de la clave criptográfica por el usuario y la autoridad de verificación. Cada PIN es almacenado por la autoridad de verificación en un formato de hashes utilizando una función hash criptográficamente segura. En otro modelo factible la etapa de codificación del PIN usando una clave criptográfica que comprende el reemplazo de cada carácter del mismo por uno correspondiente de al menos una clave de sesión usando un deslizador para ayudar a buscar una clave de sesión, siendo posible mover el mismo sobre una pluralidad de claves de sesión, permitiéndosele así al usuario buscar la clave de sesión deseada deslizando el deslizador sobre un medio que contiene la clave criptográfica, poseyendo el mismo ranuras de tamaño predefinido que causan que cada dígito de una clave de sesión caiga en una de las mismas cuando el deslizador es colocado sobre la clave de sesión.

30 **[0011]** Además, en otro modelo factible este invento proporciona un dispositivo electrónico para almacenar una o más claves de sesión utilizadas para autenticar a un usuario de un dispositivo móvil que tenga al menos un número de identificación personal (PIN), siendo tanto el PIN como la/s clave/s de sesión conocida/s sólo por el usuario y una autoridad de verificación. El usuario codifica el PIN utilizando al menos una clave de sesión y lo transfiere a la autoridad de verificación para autenticar al usuario descodificando el PIN y comprobando si el mismo coincide con un PIN almacenado correspondiente al usuario. El dispositivo electrónico se compone de: un procesador; una pantalla para mostrar al menos una clave de sesión actual; memoria para almacenar una pluralidad de claves de sesión; y al menos dos botones de navegación para acceder a la clave de sesión «anterior» o «siguiente».

- 5 [0012] El PIN consta de una secuencia de número de caracteres predefinido y la codificación del PIN mediante una clave de sesión comprende el reemplazo de cada carácter del mismo por uno correspondiente de al menos una clave de sesión. En un modelo factible cada clave de sesión consta de una secuencia de dígitos, donde cada dígito es seleccionado aleatoriamente del conjunto de números {0,1,..., 9} mediante el uso de un generador de números aleatorio seguro.
- 10 [0013] En un modelo factible la pantalla es una LCD que consta de una pantalla de 3 dígitos para proporcionar un número de clave de sesión y una pantalla de 10 dígitos para proporcionar una clave de sesión. En otro modelo factible cada clave de sesión consta de una secuencia de alfabetos, donde cada alfabeto es seleccionado aleatoriamente a partir de un alfabeto predefinido mediante un generador de alfabeto aleatorio seguro. Así mismo, en otro modelo factible el procesador solicita al usuario que elimine una clave de sesión de la memoria una vez que haya sido utilizada para codificar el PIN, lo que permite que una clave de sesión se utilice para codificar el PIN sólo una vez. El dispositivo electrónico es alimentado de una de las siguientes maneras: una fuente de alimentación y una batería, y además incluye un teclado numérico para introducir el PIN en el dispositivo electrónico, la codificación del PIN introducido mediante una clave de sesión almacenada en el dispositivo electrónico es realizada por el procesador, el PIN codificado aparece en la pantalla.
- 20

Breve descripción de los dibujos adjuntos

- 25 [0014] Este invento es descripto por medio de modelos factibles ilustrados en los dibujos adjuntos, a saber:
- [0015] FIGURA 1 muestra una lista de claves de sesión, de conformidad con un modelo factible de este invento;
- 30 [0016] FIGURA 2 ilustra una lista de claves de sesión provista de un deslizador, de conformidad con un modelo factible de este invento;
- [0017] FIGURA 3 ilustra un dongle electrónico usado para almacenar claves de sesión, de conformidad con un modelo factible de este invento; y
- 35 [0018] FIGURA 4 ilustra otro dongle utilizado para almacenar claves de sesión, de conformidad con un modelo factible de este invento.

Descripción detallada del invento

40

7

5
10
15

[0019] Este invento proporciona un dispositivo para autenticar al usuario de un dispositivo móvil como un teléfono móvil u otro dispositivo de computación personal. Este invento también proporciona una pluralidad de métodos para realizar la autenticación de un usuario remoto a través de una red de comunicación sin la instalación de software criptográfico alguno en los dispositivos de acceso y sin modificar el protocolo de comunicación predeterminado de ninguna manera. Los métodos se basan en un número de identificación personal compartido (PIN) entre el usuario y la autoridad verificadora. La autenticación se realiza haciendo que el usuario introduzca el PIN en un punto de acceso de red asociada de forma cifrada, transmitiendo el PIN cifrado y comprobando, al ser recibido por la autoridad verificadora, que los datos transmitidos pueden ser descifrados para recuperar el PIN. El cifrado es realizado por el usuario antes de introducir el PIN mediante una clave criptográfica única que se almacena por escrito y el protocolo de cifrado está diseñado para ser utilizado incluso por usuarios de bajo nivel de alfabetización.

20

[0020] Los métodos y dispositivos de autenticación descriptos son rentables y proporcionan una autenticación segura a organizaciones que operan en el comercio móvil o electrónico, transferencia de fondos en línea, otras funciones bancarias que pueden realizarse por vía electrónica y otros lugares en los cuales la autenticación de usuarios es un requisito para acceder al dispositivo.

25
30
35

[0021] La siguiente información se proporciona para permitir que una persona con habilidad ordinaria pueda practicar el invento. Los ejemplos de los modelos factibles se proporcionan únicamente con fines ilustrativos y diversas modificaciones serán evidentes para personas expertas. Los principios generales definidos en el presente documento podrán aplicarse a otros modelos factibles y aplicaciones sin apartarse del espíritu y el alcance del invento. Asimismo, la terminología y fraseología utilizadas tienen el fin de describir ejemplos de modelos factibles y no deben considerarse limitantes. Por lo tanto, se le debe conceder a este invento el alcance más amplio que abarque numerosas alternativas, modificaciones y equivalentes coherentes con los principios y características divulgados. Con fines de claridad, los detalles relativos al material técnico conocido en las áreas técnicas relacionadas con el invento no se han descrito en detalle para no opacar innecesariamente al invento.

40

[0022] Los métodos de autenticación de usuarios proporcionados por este invento requieren que cada usuario comparta un número único de identificación personal (PIN) con una autoridad de verificación. En varios modelos factibles cada PIN es una secuencia de dígitos y para fines de ilustración cada PIN descrito aquí tiene 4 dígitos. La solución proporcionada en el presente documento puede fácilmente extenderse a una configuración donde los PIN son más largos o más cortos. La

8

seguridad de la presente solución se basa en la confidencialidad de un PIN y nadie sino el legítimo usuario o la autoridad de verificación debe tener conocimiento del mismo.

5 **[0023]** Ahora el presente invento se examinará en el contexto de los modelos factibles como se ilustra en los dibujos adjuntos.

10 **[0024]** Varios modelos factibles de este invento proporcionan métodos de autenticación de usuarios que implican la generación de una clave criptográfica para cada uno. La clave criptográfica puede ser almacenada en una tarjeta de papel o en un folleto de tarjetas o usando cualquier otro medio que permita el fácil acceso a las claves o su lectura por parte del usuario. Al usuario se le entrega una copia de la clave mientras otra copia es conservada por una autoridad de verificación en forma digital. En uno de los modelos factibles cada clave está representada por una secuencia de dígitos en donde cada dígito se selecciona aleatoriamente a partir del conjunto de números {0,1, ..., 9} utilizando un generador de números aleatorios seguro. La clave criptográfica es dividida en segmentos de 10 dígitos cada uno y cada segmento se conoce como una *clave de sesión*. FIGURA 1 ilustra una lista de claves de sesión, de acuerdo a uno de los modelos factibles de este invento. Cada clave de sesión se ilustra en la FIGURA 1 se representa como un 2 por 10 tabla 102 donde la primera fila de la tabla 104 es siempre fija y contiene los dígitos 0,1,2, ..., 9 en ese orden. Los 10 dígitos en la clave de sesión se almacenan en la segunda fila 106 de la tabla 104.

25 **[0025]** Uno de los modelos factibles de este invento requiere del usuario el uso de una clave de sesión única cifrada. Se le requiere al usuario que añada a cada mensaje saliente su PIN cifrado al realizarse la codificación bajo la primera clave de sesión *no usada* en la lista de claves de sesión. En uno de los modelos factibles de este invento las claves de sesión se proporcionan a los usuarios en forma de folletos de papel. Hay un gran número de claves de sesión en cada folleto de papel, del orden de aproximadamente 100. (En las figuras, sólo se muestra una tarjeta de tal folleto.) En caso de agotamiento de todas las claves de sesión, se le emite al usuario un folleto de papel nuevo con una clave criptográfica fresca convenientemente segmentada en claves de sesión.

30 **[0026]** Con referencia a la FIGURA 1, con el fin de codificar el PIN con una clave de sesión especial, se le solicita al usuario realizar una búsqueda dígito por dígito en la tabla 102 y devolver los 4 dígitos de la clave de sesión, cuyas posiciones corresponden a los dígitos del PIN. Por ejemplo, si el PIN del usuario es 7819, primero el usuario busca el 7^{mo} dígito 108 en la primera clave de sesión 110, luego el 8^{vo} dígito 112, luego el 1^{er} dígito 114 y luego el 9^{vo} dígito 116; estos 4 dígitos juntos forman la codificación del PIN. Si el usuario está trabajando ac-

9

tualmente con la primera clave de sesión 110 que se ilustra en la FIGURA 1, el PIN cifrado consistiría del 7^{mo} dígito 108 en la clave de sesión (que es 5), seguido por el 8^{vo} dígito 110 (que es 8), seguido por el 1^{er} dígito 112 (que es 6) y seguido por el 9^{no} dígito 114 (que es 0), resultando en los dígitos 5860 como el PIN cifrado.

5

10 [0027] Si el usuario está trabajando actualmente con la segunda clave de sesión 118 que se ilustra en la FIGURA 1, y el PIN del usuario es el 7819, el PIN cifrado se obtiene convenientemente buscando entre los dígitos 7, 8, 1, 9 en la segunda tabla 120, que da los dígitos 5860 como el PIN cifrado. En uno de los modelos factibles el uso de la tarjeta de papel o folleto se implementa de modo tal que una vez que una clave de sesión se ha utilizado para la codificación, la misma es eliminada del folleto por el usuario. La eliminación de claves de sesión usadas es importante para garantizar una seguridad sólida, sin embargo, el método de este invento funciona incluso si no se implementa tal eliminación. En varios modelos factibles es importante que tanto el usuario como la autoridad de verificación realicen un seguimiento de la primera clave de sesión no utilizada en la secuencia de claves de sesión correspondientes al usuario. Esta es la clave utilizada tanto para el cifrado como para el descifrado del PIN en cada transmisión del usuario a la autoridad de verificación.

15

20

25 [0028] En diversos modelos factibles del presente invento, el usuario añade el PIN cifrado al mensaje que debe ser transmitido y envía el mensaje resultante a la autoridad de verificación, junto con su identificador (como, por ejemplo, un número de teléfono móvil). Una vez recibido el mensaje, la autoridad de verificación descifra los últimos 4 dígitos en el mensaje utilizando la copia de la clave del usuario se conserva (el descifrado consiste en realizar una búsqueda inversa en la tabla correspondiente a la clave de sesión) y comprueba si el descifrado es el mismo que el PIN del usuario. Si es así, la autenticación es exitosa, de lo contrario, no lo es.

30

35

Ejemplo del Modelo Factible # 1

40 [0029] En un modelo factible de este invento, en ciertos escenarios, el cifrado de PIN múltiples puede resultar en los mismos dígitos, es decir, múltiples PIN pueden tener la misma codificación. Esto sucedería si la clave de sesión que se utilizara tuviera dígitos repetidos provocando que dos dígitos de dos PIN diferentes se asignarían al mismo dígito cifrado. Para hacer frente a esta posibilidad, en un modelo de este invento, un PIN cifrado recibido por la autoridad de verificación puede ser descifrado como varios valores PIN de usuario. La autoridad de verificación determina si alguno de los valores de PIN obtenidos del usuario corresponde al PIN esperado. La autenticación falla sólo si ninguno de los valores de PIN obtenidos del usuario corresponde a un valor PIN esperado. En un modelo

45

50

factible, las claves de sesión son generadas de tal manera que cada clave de sesión es una permutación aleatoria de los dígitos {0,1,2, ..., 9}, recogidos uniformemente al azar para tales permutaciones. Esta selección aleatoria de dígitos de claves de sesión elimina de forma automática la posibilidad de que un cifrado sea descifrado para múltiples PIN candidatos. En diversos modelos factibles los PIN de un usuario son almacenados en forma de hash por la autoridad de verificación, mediante una función hash criptográficamente segura. El propósito de esto es asegurarse de que un atacante que logre acceder al lugar de almacenamiento de la autoridad de verificación obtenga una minúscula ventaja en la obtención de los PIN de los usuarios que están destinados a mantenerse en secreto.

Ejemplo del Modelo Factible # 2

[0030] En un modelo factible de este invento, el PIN cifrado no es numérico sino consiste en los símbolos de un alfabeto arbitrario. Por ejemplo, los PIN podrían obtenerse a partir del alfabeto inglés o de cualquier otro alfabeto legible para los usuarios finales. Las claves de sesión serían de la misma longitud que el alfabeto y consistirían en símbolos aleatorios del mismo. Para cifrar el PIN se utilizaría la misma operación de búsqueda utilizada en el caso de los dígitos descritos con referencia a la FIGURA 1.

Ejemplo del Modelo Factible # 3

[0031] En un modelo factible de este invento las claves de sesión no están representadas en forma de tablas sino como una secuencia de dígitos (o alfabetos, en el caso general). Para que el proceso de búsqueda sea fácil para el usuario, se implementa un «deslizador». FIGURA 2 ilustra una lista de claves de sesión provista con un deslizador. El deslizador 202 tiene los dígitos 0, 1, 2, ..., 9 escritos en él, convenientemente espaciados de modo que cuando se lo coloca sobre una clave de sesión 204, el '0' 206 en el deslizador 202 está situado por encima del primer dígito 208 de la clave de sesión, '1' se encuentra por encima del segunda dígito, '2' por encima del tercer dígito y así sucesivamente. El deslizador 202 es móvil pudiendo situarse tanto sobre una clave de sesión 204 como sobre otra clave de sesión 210 y ayudaría en la realización de búsquedas para todas las claves de sesión en la lista. Las claves de sesión 212 situadas sobre el deslizador 202 son las claves de sesión que se han utilizado mientras que las 214 situadas debajo del deslizador son las claves de sesión no utilizadas. En un modelo factible, el deslizador 202 mismo puede ser un objeto de papel o puede estar hecho de otros materiales, y puede tanto ser añadido a un folleto de papel de claves de sesión o puede estar separado. En un modelo factible el deslizador tiene 10 ranuras del tamaño adecuado de modo que al situárselo sobre una clave de sesión, cada dígito de la clave de sesión cae en una de las ranuras.

Ejemplo del Modelo Factible # 4

5
10
15

[0032] En un modelo factible de este invento, cuando las transacciones basadas en PIN son muy frecuentes y las claves de sesión expiran pronto, las claves de sesión son almacenadas electrónicamente en lugar de en papel. FIGURA 3 ilustra un dongle electrónico utilizado para almacenar claves de sesión, de acuerdo con un modelo factible de este invento. Cada usuario tiene un dongle electrónico 302 que comprende un procesador 304 y una pantalla LCD 306 que muestra la clave de sesión actual. La pantalla LCD 306 comprende una pantalla de 3 dígitos para proporcionar un número de clave de sesión y una pantalla de 10 dígitos para proporcionar una clave de sesión. El dongle electrónico 302 está equipado con memoria de sólo lectura (ROM) 308 o una memoria flash que almacena todas las claves de sesión proporcionadas al usuario. Los botones de navegación 310 y 312 pueden ser utilizados para acceder a una clave de sesión «anterior» o «siguiente» respectivamente. Las claves de sesión se pueden borrar de la memoria a medida y mientras se van utilizando para el cifrado. El dongle 302 puede ser alimentado por una fuente de poder o batería 314.

20
25

[0033] En un modelo factible, el dongle está equipado con un teclado numérico y la operación de cifrado en sí se lleva a cabo por el mismo, tornando así a la interfaz de usuario en una aún más accesible a los usuarios analfabetos. FIGURA 4 ilustra otro dongle utilizado para almacenar claves de sesión, de conformidad con un modelo factible de este invento. Además de los componentes descritos con referencia a la FIGURA 4, el dongle 402 consta de un conjunto de 10 claves 404 para introducir el número de PIN de un usuario. El PIN introducido se codifica utilizando una clave de sesión y el método de búsqueda descrito con referencia a la FIGURA 1 electrónicamente por el procesador del dongle 502, y el PIN cifrado aparece en pantalla LCD.

30
35
40

[0034] De ahí que este invento proporciona un interfaz basado en papel para almacenar una larga secuencia de claves de sesión criptográfica y utiliza métodos seguros para realizar el cifrado de PIN. La invento también proporciona un equipo electrónico de bajo costo para realizar el cifrado. La presente invento también proporciona un método para realizar el cifrado de PIN, o más generalmente, de cortos mensajes numéricos, cuyas operaciones de cifrado y descifrado son fáciles de implementar y puede ser realizada por personas de alfabetización muy limitada y habilidades numéricas. En consecuencia, se proporciona un método para el cifrado de mensajes en la capa «interfaz de usuario» (por encima de la capa de aplicación) del protocolo de comunicación, es decir, incluso antes de que sean recibidos mensajes por una aplicación de software, ya han sido cifrados por el usuario. Esto hace que el cifrado sea más robusto frente a posibles programas malignos en la red de comunicación. Por lo tanto, el presente invento se basa en un esquema criptográfico simple como el «libreta de un solo uso» (del inglés

«OTP») para diseñar un método de cifrado que puede ser implementado en su totalidad por seres humanos y sin ningún tipo de soporte de software.

[0035] Aunque los ejemplos de modelos factibles del presente invento son descriptos e ilustrados aquí, se apreciará que son meramente ilustrativos. Los expertos en la técnica entenderán que se podrían realizar diversos cambios en forma y detalle sin apartarse u ofender el espíritu y el alcance del invento.

3

Lo que se reivindica es que:

- 5
1. Un método para un usuario de un dispositivo móvil que sea autenticado por una autoridad de verificación, haciendo uso de al menos un número de identificación personal (PIN) y al menos una clave criptográfica, siendo tal PIN y clave criptográfica conocidos sólo por el usuario y la autoridad de verificación, y comprendiendo la clave criptográfica al menos una clave de sesión, comprendiendo tal método al menos las siguientes etapas:
- 10
- a. la codificación del PIN por parte del usuario mediante el uso de al menos una clave de sesión;
 - b. la transferencia por parte del usuario del PIN codificado a una dirección predefinida de la autoridad de verificación a través del dispositivo móvil;
 - c. la decodificación del PIN por parte de la autoridad de verificación mediante el uso de la clave criptográfica, y
 - d. la autenticación por parte de la autoridad de verificación del usuario si el PIN decodificado coincide con un PIN almacenado correspondiente al mismo.
- 15
2. El método como se lo reivindica en la reivindicación 1 en la cual el dispositivo móvil es un teléfono celular.
- 20
3. El método como se lo reivindica en la reivindicación 1 en el que el dispositivo móvil es un dispositivo de computación.
- 25
4. El método como se lo reivindica en la reivindicación 1 en el que el PIN comprende una secuencia de número de caracteres predefinida, siendo el PIN conocido sólo por el usuario y la autoridad de verificación.
- 30
5. El método como se lo reivindica en la reivindicación 1 en la que el paso de codificar el PIN mediante el uso de una clave criptográfica comprende la sustitución de cada carácter del PIN por un carácter correspondiente de al menos una clave de sesión.
- 35
6. El método como se lo reivindica en la reivindicación 1 en la cual la clave criptográfica comprende una secuencia de dígitos, de la cual cada dígito se selecciona aleatoriamente a partir del conjunto de números {0,1, ..., 9} utilizando un generador de números aleatorios seguro, estando la clave criptográfica dividida en una o más claves de sesión que contienen 10 dígitos cada uno.
- 40
7. El método como se lo reivindica en la reivindicación 1 en la que el usuario es provisto de una clave criptográfica que comprende una pluralidad de claves de sesión, siendo cada clave de sesión utilizada para autenticar al usuario sólo

una vez, siendo la clave criptográfica proporcionada en la forma de un folleto de papel.

- 5 8. El método como se lo reivindica en la reivindicación 1 en la que la clave criptográfica comprende una secuencia de alfabetos, de la cual cada alfabeto es seleccionado aleatoriamente a partir de un alfabeto predefinido utilizando un generador de alfabetos aleatorios seguro, estando la clave criptográfica dividida en una o más claves de sesión que comprenden un número predefinido de alfabetos cada una, siendo uno o más códigos de transformación presentados al usuario en una pluralidad de estilos de presentación.
- 10 9. El método como se lo reivindica en la reivindicación 1 en la que una clave de sesión utilizada para codificar el PIN una vez, es retirada de la clave criptográfica por el usuario y la autoridad de verificación.
- 15 10. El método como se lo reivindica en la reivindicación 1 en donde al menos un PIN es almacenado por la autoridad de verificación en un formato hash utilizando una función hash criptográficamente segura.
- 20 11. El método como se lo reivindica en la reivindicación 1 en la que la etapa de la codificación del PIN mediante el uso de una clave criptográfica comprende la sustitución de cada carácter del PIN por un carácter correspondiente de al menos una clave de sesión utilizando un deslizador para ayudar a buscar una clave de sesión, estando el deslizador capacitado para moverse sobre una pluralidad de claves de sesión, permitiendo así al usuario buscar una clave de sesión deseada deslizando al deslizador sobre un medio que contiene la clave criptográfica, comprendiendo el deslizador ranuras de tamaño predefinido, causando que cada dígito de una sesión caiga en una de las ranuras cuando el deslizador se coloca sobre la clave de sesión.
- 25 30 12. Un dispositivo electrónico para almacenar una o más claves de sesión utilizadas para la autenticación de un usuario de un dispositivo móvil que tenga al menos un número de identificación personal (PIN), siendo tanto el PIN como la única o muchas claves de sesión conocidas sólo por el usuario y una autoridad de verificación, el usuario codifica el PIN utilizando al menos una clave de sesión y transfiere el PIN codificado a la autoridad de verificación para la autenticación del usuario mediante la decodificación del PIN y verificando si el PIN decodificado coincide con un PIN almacenado correspondiente al usuario, el dispositivo electrónico comprende:
 - 35 a. un procesador;
 - 40 b. una pantalla para presentar al menos una clave de sesión actual;
 - c. memoria para almacenar una pluralidad de claves de sesión, y

15

- d. por lo menos dos botones de navegación para acceder a una clave de sesión «anterior» o «siguiente».

- 5 13. El dispositivo electrónico tal como se lo reivindica en la reivindicación 12 en donde el PIN comprende una secuencia de número de caracteres predefinido.
- 10 14. El dispositivo electrónico tal como se lo reivindica en la reivindicación 12 en donde la codificación del PIN mediante una clave de sesión comprende la sustitución de cada carácter del PIN por el carácter correspondiente de al menos una clave de sesión.
- 15 15. El dispositivo electrónico tal como se lo reivindica en la reivindicación 12 en donde cada clave de sesión comprende una secuencia de dígitos, en donde cada dígito se selecciona aleatoriamente a partir del conjunto de números {0,1, ..., 9} utilizando un generador de números aleatorios seguro.
- 20 16. El dispositivo electrónico tal como se lo reivindica en la reivindicación 12 en donde la pantalla es una LCD que comprende una pantalla de 3 dígitos para proporcionar un número clave de sesión y una pantalla de 10 dígitos para proporcionar una clave de sesión.
- 25 17. El dispositivo electrónico tal como se lo reivindica en la reivindicación 12 en donde cada clave de sesión comprende una secuencia de alfabetos, en donde cada alfabeto se selecciona aleatoriamente a partir de un alfabeto predefinido mediante un generador de alfabeto aleatorio seguro.
- 30 18. El dispositivo electrónico tal como se lo reivindica en la reivindicación 12 en donde el procesador solicita al usuario que elimine una clave de sesión de la memoria una vez que la misma se ha utilizado para codificar el PIN, lo que permite que una clave de sesión sea utilizada para codificar el PIN sólo una vez.
- 35 19. El dispositivo electrónico tal como se lo reivindica en la reivindicación 12 siendo alimentado por una: fuente de energía y una batería.
- 20. El dispositivo electrónico tal como se lo reivindica en la reivindicación 12 comprendiendo además un teclado numérico para introducir el PIN en el dispositivo electrónico, la codificación del PIN introducido mediante el uso de una clave de sesión almacenada en el dispositivo electrónico que funciona por el procesador, mostrándose al PIN codificado en la pantalla.

RESUMEN

Este invento describe un método para que una autoridad de verificación autentifique a un usuario de un dispositivo móvil, utilizando al menos un número de identificación personal (PIN) y al menos una clave criptográfica, de modo tal que el PIN y la clave criptográfica sólo sean conocidos por el usuario y la autoridad de verificación. La clave criptográfica tiene al menos una clave de sesión. En primer lugar, el usuario codifica el PIN mediante el uso de al menos una clave de sesión y luego transfiere el PIN codificado a una dirección predefinida de la autoridad de verificación a través del dispositivo móvil. A continuación, la autoridad de verificación decodifica al PIN mediante la clave criptográfica y autentifica al usuario si el PIN descodificado coincide con un PIN almacenado correspondiente al usuario.

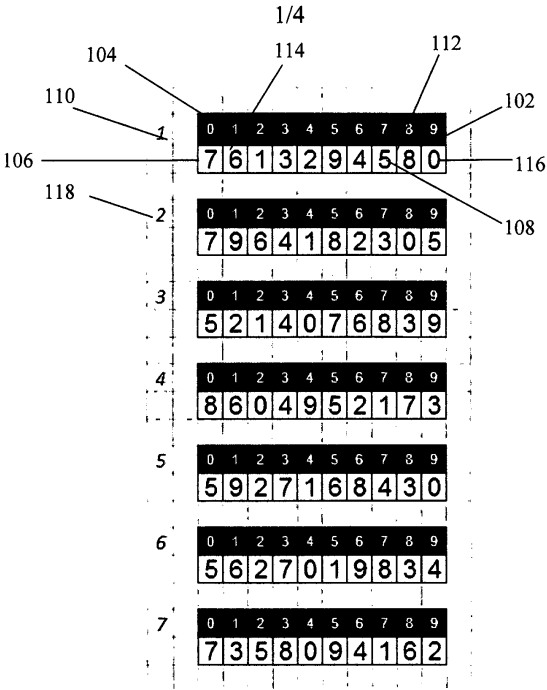


FIG. 1

17

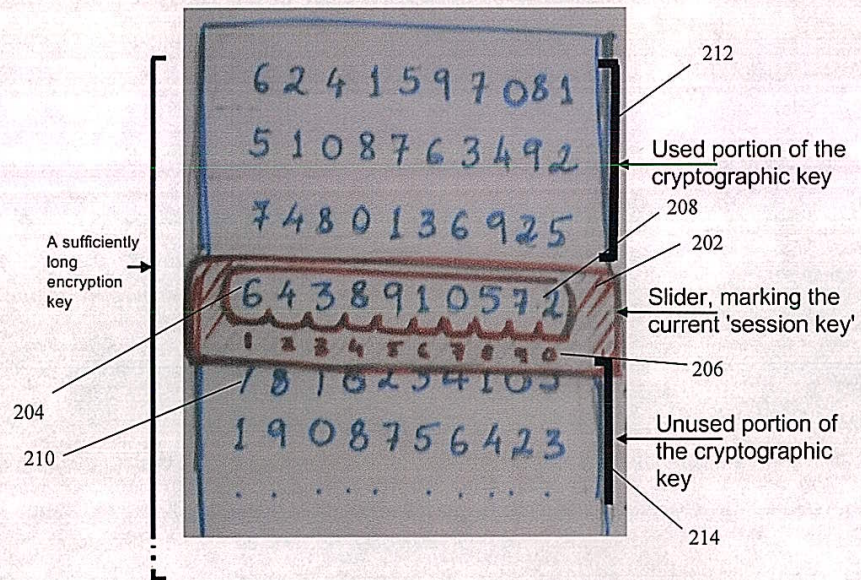


FIG. 2

18

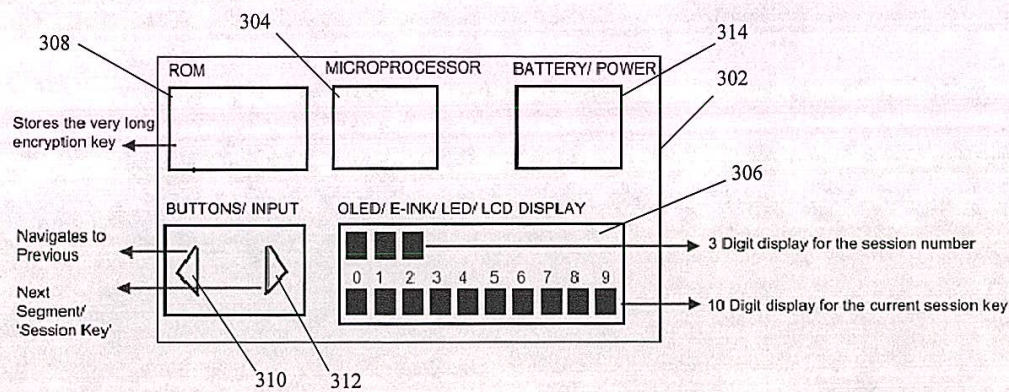


FIG. 3

19

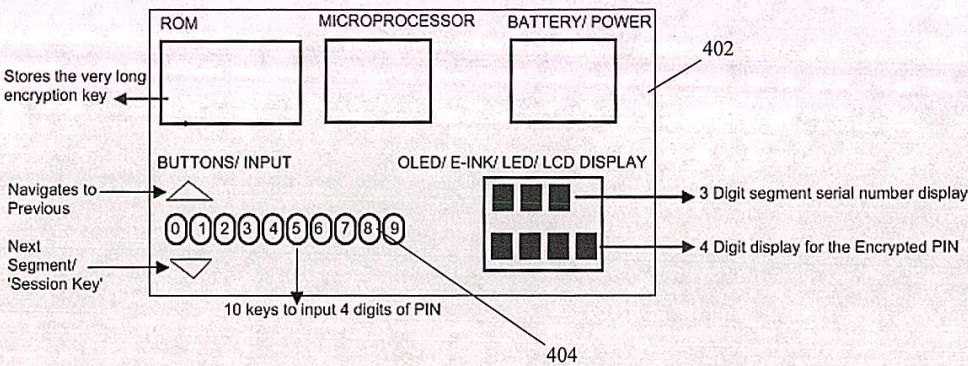


FIG. 4

20

A sufficiently long encryption key →	Una clave cifrada suficientemente larga.
<u>Used</u> portion of the cryptographic key	Porción <u>usada</u> de la clave criptográfica.
<u>Slider</u> , marking the current 'session key'	<u>Deslizador</u> , destacando la clave de sesión actual.
<u>Unused</u> portion of the cryptographic key	Porción <u>no utilizada</u> de la clave criptográfica.
Stores the very long encryption key ←	Almacena la clave de cifrado muy larga
Navigates to Previous	Navega al Anterior
Next Segment/ 'Session Key'	Siguiente Segmento/Clave de sesión
10 Digit display for the current session key	Pantalla de 10 dígitos de la clave de sesión actual
3 Digit display for the session number	Pantalla de 3 dígitos para el número de sesión
BUTTONS/ INPUT	BOTONES/ENTRADA
OLED/ E-INK/ LED/ LCD DISPLAY	OLED=Object Linking & Embedding (La vinculación e incrustación de objetos) E-LINK= Electronic Link (Vínculo electrónico) LED=Light-Emitting Diode (Diodo emisor de luz) LCD= Liquid Cristal Display (Pantalla de cristal líquido)
ROM	ROM= Read Only Memory (Memoria de solo lectura)
MICROPROCESSOR	Micro procesador
BATTERY/ POWER	BATERÍA/ENERGÍA
Stores the very long encryption key ←	Almacena la clave de cifrado muy larga
Navigates to - Previous	Navega al Anterior

22

Next Segment/ — 'Session Key'	Siguiente Segmento/Clave de sesión
BUTTONS/ INPUT	BOTONES/ENTRADA
OLED/ E-INK/ LED/ LCD DISPLAY	OLED=Object Linking & Embedding (La vinculación e incrustación de objetos) E-LINK= Electronic Link (Vínculo electrónico) LED=Light-Emitting Diode (Diodo emisor de luz) LCD= Liquid Cristal Display (Pantalla de cristal líquido)
10 keys to Input 4 digits of PIN	10 claves para introducir los 4 dígitos de un PIN
4 Digit display for the Encrypted PIN	Pantalla de 4 dígitos para el PIN cifrado.
3 Digit segment serial number display	Pantalla de segmento de número serial de 3 dígitos
ROM	ROM= Read Only Memory (Memoria de solo lectura)
MICROPROCESSOR	Micro procesador
BATTERY/ POWER	BATERÍA/ENERGÍA

Castillo Grau & Asociados

ABOGADOS
APARTADO AEREO 251473
BOGOTA, COLOMBIA

25

25

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
NIT : 800.176.089-2
- / -

 Industria y Comercio SUPERINTENDENCIA	RECIBO DE CAJA	No. 12 - 100143
		Bogotá D.C., Octubre 01 de 2012 - 15:48:33

RECIBIDO DE : CASTILLO GRAU & ASOCIADOS LTDA. NI 800.098.704

*** Soporte del Pago ***					
TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	VR PAGO
CONSIGNACION	BANCO DE BOGOTA	062754387	409420712	01/10/2012	8.300.000.00

*** Conceptos Pagados ***			
CANT. RENTISTICO	CONCEPTO	Vr. UNDITARIO	Vr. CONCEPTO
1 50005-01-01 SOLICITUDES	1 TRAMITES DE SOL. DE PATENTE DE INVENCIÓN	590.000.00	590.000.00
			\$590.000.00
		=====	

SON: **QUINIENTOS NOVENTA MIL PESOS MONEDA CORRIENTE**

Responsable: _____

Recibo de Caja Aplicado al Expediente No. _____

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 12-171852- -00000-0000

Fecha: 2012-10-01 16:10:46 Dep. 2020 DIR.NUEVASCR
Tra. 11 PATENTEIYII Eve: 378 FASENACIONALI
Act. 411 PRESENTACION Folios: 26

25



No. 12-171852- -00000-0000

Fecha: 2012-10-01 16:10:46 Dep. 2020 DIR.NUEVAS
Tra. 11 PATENTEIYII Eve: 378 FASENACIONAL
Act. 411 PRESENTACION Folios: 25

PATENTE DE INVENCION

☒

MODELO DE UTILIDAD

☐

Art 33 Decisión 486/00

☒	Indicación que se solicita una patente.
☒	Datos de identificación del solicitante o de la persona que presenta la solicitud
☒	Descripción de la invención
☒	Dibujos de ser estos pertinentes
☒	Comprobante de pago de las tasas establecidas (De ser el caso formato de descuento)
Completa	☒
Incompleta	☐

PATENTE DE INVENCION PCT

☐

MODELO DE UTILIDAD PCT

☐

Art.33 Decisión 486/00, Circular Única

☐	Indicación que se solicita una PCT
☐	Copia de la solicitud en español, tal como fue presentada inicialmente (capítulo descriptivo, reivindicatorio, resumen)
☐	Dibujos de ser estos pertinentes
☐	Comprobante de pago de las tasas establecidas (de ser el caso formato de descuento)
Completa	☐
Incompleta	☐

DISEÑO INDUSTRIAL

☐

(Art. 119 Decisión 486/00)

☐	Indicación que se solicita Diseño industrial
☐	Datos de identificación del solicitante o de la persona que presenta la solicitud
☐	Representación gráfica y fotográfica del Diseño industrial o muestra del material que incorpora el diseño
☐	Comprobante de pago de las tasas establecidas
Completa	☐
Incompleta	☐

ESQUEMA DE TRAZADO

☐

(Art. 92 Decisión 486/00)

☐	Indicación que se solicita un esquema de trazado
☐	Datos de identificación del solicitante o de la persona que presenta la solicitud
☐	Representación gráfica de un esquema de trazado
☐	Comprobante de pago de las tasas establecidas
Completa	☐
Incompleta	☐