

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO	
RAD: 12-171852- -5	FECHA: 2013-12-10 15:37:58
DEP: 2020 DIRECCION DE NUEVAS CREACIONES	EVE: 378 FASE NACIONAL INCLUIDO CAPITULO I
TRA: 11 PCT-PATENTE DE INVENCION CAPITULOS I Y II	FOLIOS: 8
ACT: 519 PRESENTACION	

DIRECCIÓN DE NUEVAS CREACIONES

2020
Bogotá, D.C.,

Abogado(a)/Señor(a)
LUIS FELIPE CASTILLO GIBSON

Asunto: Radicación: 12-171852- -5
Trámite: 11
Evento: 378
Actuación: 519
Oficio: 22780
Folios: 8

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/IN2011/000128				
Fecha de Presentación Internacional	01/03/2011				

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° 12-171852-00000-0000	01/Octubre/2012
Reivindicaciones:	Rad. N° 12-171852-00000-0000	01/Octubre/2012
Dibujos:	Rad. N° 12-171852-00000-0000	01/Octubre/2012
Prioridad:	IN 451/DEL/2010	02/Marzo/2010

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 10.

Título de la solicitud: “Procedimiento y dispositivo de autenticación” (ver página 1 del radicado N° 12-171852-00000-0000).

El problema planteado en esta solicitud consiste en la necesidad de suministrar un método y un dispositivo para autenticar un usuario en el uso de transacciones bancarias por medio de dispositivos móviles, que proporcione un sistema de seguridad robusto en cuanto a la autenticación del usuario, implementado en un equipo móvil de baja gama.

Para resolver este problema técnico, la solicitud en estudio proporciona 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 solo por el usuario y la autoridad de verificación, y comprendiendo la clave criptográfica al menos una clave de sesión, que comprende los pasos de: la codificación del PIN por parte del usuario mediante el uso de al menos una clave de sesión; la transferencia por parte del usuario del PIN codificado a una dirección predefinida por la autoridad de verificación a través del dispositivo móvil; la decodificación del PIN por parte de la autoridad de verificación mediante el uso de la clave criptográfica, y la autenticación por parte de la autoridad de verificación de usuario si el PIN decodificado coincide con un PIN almacenado correspondientemente al mismo. De igual manera, suministra un dispositivo electrónico para almacenar uno o más claves de sesión utilizadas para autenticación de un usuario de un dispositivo móvil, que comprende: un procesador, una pantalla, una memoria y por lo menos dos botones de navegación.

El objeto de la presente solicitud se relaciona con la Clasificación Internacional de Patentes (CIP): H 04 W 12/04.

4. De la solicitud de patente

Reivindicaciones (Art 30 D 486, Art 22 PCT)

Las reivindicaciones 1, 5, 6, 8 y 10 a 12 no son claras porque los términos: “*al menos*”, “*una o más*” y “*por lo menos*” 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.

Las reivindicaciones 1 a 3, 12 y 19 no son claras porque los términos: “*dispositivo móvil*”, “*un procesador*” y “*una fuente de energía*” son generales, por lo tanto no permiten establecer la diferencia y el aporte realizado por la invención frente al estado de la técnica.

Las reivindicaciones 4, 12, 14, 16, 18 y 20 no son claras porque caracterizan la invención por sus resultados a obtener así, “*siendo el PIN conocido solo por el usuario y la autoridad de verificación*”, “*para presentar al menos una clave de sesión actual*”, “*para almacenar una pluralidad de claves de sesión*”, “*para acceder a una clave de sesión <<anterior>> o <<siguiente>>*”, “*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*”, “*para proporciona un numero de clave de sesión*”, “*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*”, “*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 solo una vez*”, “*siendo alimentado por una fuente de energía y una batería*”, “*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” 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.

Las reivindicaciones 2 y 3 no son claras porque se encuentra reivindicando materia propia de un producto dentro de la categoría de procedimiento, debido a que “un dispositivo móvil” es considerado una característica técnica tangible y no un paso de un procedimiento.

Las reivindicaciones 13, 15 y 17 no son claras porque la materia reclamada no es considerada de carácter técnico como tal, por el contrario especifican parámetros de: “PIN” y “clave de sesión”, que son considerados de carácter intangible.

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: marzo 02 de 2010 y se encontraron los siguientes documentos que anticipan el objeto de esta solicitud:

Ítem	Documento	Título	Fecha de Publicación
D1	US 4,423,287	“End-to-end encryption system and method of operation”	27/Diciembre/1983
D2	WO 2005041608	“Method of user authentication”	06/Mayo/2005

El documento D1¹ divulga un sistema de cifrado de extremo a extremo eficiente, incluyendo los procedimientos de gestión de claves para proporcionar una comunicación segura, datos financieros entre un usuario del sistema en uno de una pluralidad de terminales de transacción de una pluralidad de instituciones adquirentes y uno de una pluralidad de instituciones emisoras, con elementos seleccionados de los datos, siendo cifrados/descifrados, y se procesan utilizando una clave de sesión la cual que es igualmente cifrada con claves maestras y enviadas eficiente, junto con los segmentos específicos de la solicitud y un mensaje de respuesta (Pág. 1, Fl. 1, resumen).

1 <https://docs.google.com/viewer?url=patentimages.storage.googleapis.com/pdfs/US4423287.pdf>

El documento D2² divulga un método de autenticación de usuario en una red que comprende un terminal móvil, un proveedor de servicios y un servidor de autenticación. El terminal móvil tiene una tarjeta inteligente con funciones de seguridad y la información específica de usuario/equipo. En el método, el usuario ofrece (3) información sobre la identidad del proveedor de servicios como respuesta a una solicitud (1) para el uso de un servicio proporcionado por el proveedor de servicios. La información de identidad dada por el usuario es enviado (4) desde el proveedor de servicios al servidor de autenticación, que genera (5) un número aleatorio, que se envía (6) a la tarjeta inteligente del terminal móvil (Pág. 1, Fl. 1, resumen).

6. Examen de Patentabilidad (Art 14 D486)

Nivel inventivo (Art18 D486)

La reivindicación 1 consiste en “*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...*” (Ver página 13 del radicado N° 12-171852-00000-0000).

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

Características esenciales	D1	D2
La codificación del PIN por parte del usuario mediante el uso de una clave de sesión.	La clave de sesión se descifra con la primera llave maestra, y el número de identificación personal PIN se cifra mediante la clave de sesión y el algoritmo estándar de cifrado de datos (Pág. 14, Col. 6, líneas 55 a 58).	No menciona.
La transferencia por parte del usuario del PIN codificado a una dirección predefinida de la autoridad de verificación a través del dispositivo móvil.	La terminal de transacción (10) calcula entonces un primer mensaje del código de autenticación (MAC1) en los datos críticos mediante la clave de sesión. Sólo ciertos elementos de datos, como el PIN, necesitan ser mantenidos en secreto por el cifrado durante la transmisión de un mensaje desde el terminal de transacciones a través de la red de intercambio para el emisor (Pág. 14, Col. 6, línea 66 a Pág. 15, Col. 7, línea 3). El terminal de transacción (10) envía a una estación asociada de adquirente (12) un mensaje que comprende el PIN cifrado, el MAC1 y otros datos de la transacción (Pág. 15, Col. 7, líneas 40 a 42). Los datos se reciben en la estación adquirente (12) conectado a ese terminal de transacción en particular. La estación (12) podría típicamente ser la sede o sucursal de la entidad financiera que controla el terminal de transacciones (10) (Pág. 15, Col. 7, líneas 52 a 56).	El método presentado se lleva a cabo en una red que comprende un usuario con su terminal móvil, un servidor de autenticación y un proveedor de servicios (Pág. 7, Fl. 9, líneas 14 y 15). En el paso 1 el usuario envía una solicitud de un servicio a un proveedor de servicios de su terminal móvil. Se supone que el terminal móvil tiene una conexión a Internet a través de por ejemplo, el Protocolo de Aplicación Inalámbrica (WAP), una interfaz y por lo tanto pueden comunicarse con el proveedor de servicios. Esto puede tener lugar por ejemplo, haciendo clic en alguna página de inicio de Internet del proveedor de servicios, lo que provoca una solicitud del mensaje para el servicio que se enviará. Un escenario más habitual sería que el usuario envía esta solicitud de su ordenador personal (PC) (Pág. 8, Fl. 10, líneas 1 a 7).
La decodificación del PIN por parte de la autoridad verificación mediante el uso de la clave criptográfica.	El emisor (20) incluye un procesador de datos principal y la base de datos (22). También puede tener un módulo de seguridad (24). El emisor (20) recibe el mensaje cifrado de la estación de conmutación de red (16). Dentro del	No menciona.

2 <http://patentscope.wipo.int/search/en/WO2005041608>

	módulo de seguridad (24), descifra la clave de sesión mediante una tercera clave maestra y descifra el PIN utilizando la clave de sesión ahora descifrada. Además, utilizando la clave de sesión, el emisor vuelve a calcular MAC1 y lo verifica (Pág. 15, Col 8, líneas 41 a 48). Entonces entrado en la parte de la memoria (34) frente a los datos de la red de intercambio. Estos datos incluyen una clave única criptográfica cifrada, que corresponde a la clave de sesión, la información de tipo de cifrado, los datos de formato de cifrado del PIN, y caracteres de relleno (Pág. 16, Col. 10, líneas 37 a 42).	
La autenticación por parte de la autoridad de verificación del usuario si el PIN decodificado coincide con un PIN almacenado correspondientes al mismo.	Con el número de cuenta primaria PAN, el emisor recupera el PIN asociado con el número de cuenta primaria PAN de la base de datos 22. Este PIN es generalmente codificado en una clave de base de datos. El PIN introducido por el usuario se cifra también en la clave de base de dato, y los dos se comparan para la verificación de la PIN introducido por el usuario. El emisor 20 entonces especifica un código de autorización, como "autorizar" o "negar" (la transacción), y genera un mensaje de retorno (Pág. 15, Col 8, líneas 48 a 57).	No menciona.

Los documentos D1 y D2 se consideran el estado de la técnica cercano a la invención definida en la reivindicación 1 porque divulgan un sistema de cifrado de extremo a extremo eficiente, incluyendo los procedimientos de gestión de claves para proporcionar una comunicación segura, datos financieros entre un usuario del sistema en uno de una pluralidad de terminales de transacción de una pluralidad de instituciones adquirentes y uno de una pluralidad de instituciones emisoras, con elementos seleccionados de los datos, siendo cifrados/descifrados, y se procesan utilizando una clave de sesión la cual que es igualmente cifrada con claves maestras y enviadas eficiente, junto con los segmentos específicos de la solicitud y un mensaje de respuesta (Pág. 1, Fl. 1, resumen); y un método de autenticación de usuario en una red que comprende un terminal móvil, un proveedor de servicios y un servidor de autenticación. El terminal móvil tiene una tarjeta inteligente con funciones de seguridad y la información específica de usuario/equipo. En el método, el usuario ofrece (3) información sobre la identidad del proveedor de servicios como respuesta a una solicitud (1) para el uso de un servicio proporcionado por el proveedor de servicios. La información de identidad dada por el usuario es enviado (4) desde el proveedor de servicios al servidor de autenticación, que genera (5) un número aleatorio, que se envía (6) a la tarjeta inteligente del terminal móvil (Pág. 1, Fl. 1, resumen); correspondientemente.

La diferencia entre la invención, definida en la reivindicación 1 y el procedimiento de D1 consiste en que no menciona el uso de un dispositivo móvil.

La diferencia entre la invención, definida en la reivindicación 1 y el procedimiento de D2 consiste en que no menciona los pasos de: la codificación del pin por parte del usuario mediante el uso de una clave de sesión, la trasferencia por parte del usuario del pin codificado a una dirección predefinida de la autoridad de verificación, la decodificación del pin por parte de la autoridad verificación mediante el uso de la clave criptográfica y la autenticación por parte de la autoridad de verificación del usuario si el pin decodificado coincide con un pin almacenado correspondientes al mismo.

El efecto que logra el incluir el uso de un dispositivo móvil es que permite ejecutar una verificación de autorización.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: “¿cómo modificar el procedimiento conocido en D1 para implementarlo mediante un dispositivo móvil?”.

Sin embargo, la utilización de un dispositivo móvil para realizar una verificación de autorización, ya está divulgada en el documento D2 que se refiere a un método que se lleva a cabo en una red que comprende un usuario con su terminal móvil, un servidor de autenticación y un proveedor de servicios (Pág. 7, Fl. 9, líneas 14 y 15).

En el paso 1 el usuario envía una solicitud de un servicio a un proveedor de servicios de su terminal móvil. Se supone que el terminal móvil tiene una conexión a Internet a través de por ejemplo, el Protocolo de Aplicación Inalámbrica (WAP), una interfaz y por lo tanto pueden comunicarse con el proveedor de servicios. Esto puede tener lugar por ejemplo, haciendo clic en alguna página de inicio de Internet del proveedor de servicios, lo que provoca una solicitud del mensaje para el servicio que se enviará. Un escenario más habitual sería que el usuario envía esta solicitud de su ordenador personal (PC) (Pág. 8, Fl. 10, líneas 1 a 7).

En consecuencia, la persona del oficio normalmente versada en la materia, incluiría el dispositivo móvil del documento D2 en el procedimiento divulgado en el documento D1 para llegar así al objeto de la reivindicación 1 de la solicitud. Por lo cual se considera obvia.

Las reivindicaciones dependiente 2 y 3 no mencionan alguna característica que haga inventivo el método de la reivindicación 1, debido a que, divulgan las mismas características técnicas de la reclamación independiente o se encuentran redactadas en términos de usos, resultados y/o características no técnicas. Por lo tanto, no se consideran inventivas.

Asimismo, los documentos D1 y D2 divulgan las características de las reivindicaciones dependientes así:

- Reivindicación 4, 6: El computo del código de autenticación de mensaje MAC comprende una concatenación de determinados datos (160) como, el tipo de mensaje, el número de transacción, el número de cuanta primario PAN, el PIN cifrado, la fecha, el tiempo, otros datos y el número cero de relleno para rellenar la última agrupación de datos de 64 bits. Algunos de estos datos pueden ser alfabético, algunos pueden ser numéricos, algunos pueden ser en forma hexadecimal (D1, Pág. 19, Col. 15, líneas 39 a 45).
- Reivindicación 5 a 8, 11: Entonces entrado en la parte de la memoria (34) frente a los datos de la red de intercambio. Estos datos incluyen una clave única criptográfica cifrada, que corresponde a la clave de sesión, la información de tipo de cifrado, los datos de formato de cifrado del PIN, y caracteres de relleno (D1, Pág. 16, Col. 10, líneas 37 a 42).
- Reivindicación 9: Una de las ventajas importantes de un sistema de cifrado de extremo a extremo, a diferencia de otros tipos de cifrado, es que se garantiza que las claves en una sesión en tiempo de todos los datos cifrados y MAC será diferente incluso para transacciones idénticas. Por lo tanto, se excluyen los datos de sustitución, la sustitución de PIN, y los ataques de tipos de mensaje-replay adversarios. Además, se ofrece potencialmente más seguridad contra los ataques de tipo de análisis estadístico. Una ventaja principal del sistema de cifrado de extremo a extremo en la actualidad es la facilidad y economía con la que estas claves de sesión se distribuyen de forma segura y eficiente. No se requiere ninguna clave de solicitud de clave o de transmisión de mensajes especiales. Otra

ventaja significativa es que el sistema también elimina los requisitos para el cifrado y re-cifrado de datos críticos, y re-cálculo de los MAC en todos los nodos intermedios. Por lo tanto, la vulnerabilidad potencial a los ataques sofisticados en casa se reduce, el mensaje de procesamiento y los requisitos de tiempo de computadora se reducen al mínimo, y el requisito para cualquier proceso de seguridad en línea en la instalación adquirente es eliminado (D1, Pág. 13, Col. 4, línea 62 a Pág. 14, Col. 5, línea 15).

- Reivindicación 10: Los algoritmos de hash acepta cualquier cantidad de datos como entrada y produce un valor hash como salida. Las longitudes de salida son de 160 bits (20 bytes) para SHA- 1 y 128 bits (16 bytes) para MD 5. El valor hash de salida también es comúnmente llamado un compendio mensajes. El proceso hash es de una sola vía y no es posible derivar la entrada original a partir de la síntesis del mensaje. Un proceso hash no puede ser revertido. Los dígitos de los mensajes son la base para la mayoría de los estándares de firma digital (D2, Pág. 4, Fl. 6, líneas 3 a 9).

7. Conclusión

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

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	US 4,423,287	1 a 11	Nivel inventivo
D2	WO 2005041608	1 a 11	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 del día siguiente 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 2013-12-17

Elaboró: Diego Gonzalez Castillo
Revisó: Sonia Andrea Diaz Pirazan