

**Señores**

**DIRECCIÓN DE NUEVAS CREACIONES**

**SUPERINTENDENCIA DE INDUSTRIA Y COME...**

**Bogotá, D.C.**

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



**No. 12-171852-00007-0000**

Fecha: 2014-04-29 15:30:54  
Tra. 11 PATENTEIYII  
Act. 523 RESPUESTA

Dep. 2020 DIR.NUEVASCR  
Eve: 378 FASENACIONALI  
Folios: 11

Re.: Código 011-378-444

Expediente No. 12-171.852

Fase nacional de Solicitud

de Patente PCT

**EKO INDIA FINANCIAL SERVICES**

**PVT. LTD.**

En relación con el expediente de la referencia y dando cumplimiento a la última providencia recaída sobre este asunto por medio del presente escrito me permito manifestarles lo siguiente:

1. Siguiendo precisas instrucciones de mi representada adjunto a este escrito me encuentro presentando un nuevo capítulo reivindicatorio, el cual ha sido revisado y corregido.
2. En la presente respuesta, las reivindicaciones 1-2, 4-12, 14, 16, y 18-20 han sido modificadas, la reivindicación 3 ha sido cancelada, y se ha añadido una nueva reivindicación 21. No se ha añadido otro objeto de la invención. El respaldo para algunas de las modificaciones se puede encontrar en los párrafos [0019] y [0028] de la solicitud. Una vez ingresadas las modificaciones, las reivindicaciones 1-2, 4-21 permanecerán en estudio en la presente solicitud, de las cuales las reivindicaciones 1, 12, y 21 son independientes.
3. D1 y D2, solos o en combinación, no enseñan, revelan ni sugieren las características citadas de las reivindicaciones independientes modificadas 1 y 12  
El Examinador no aplica las combinaciones de antecedentes que incluyen todas

las características citadas de las reivindicaciones independientes modificadas 1 y 11. Los Solicitantes respetuosamente aseveran que la presente invención, tal como está consignada en las reivindicaciones independientes modificadas 1 y 11 es patentable por sobre los antecedentes citados solos o en combinación.

Cada una de las reivindicaciones independientes modificadas 1 y 11 ahora cita, entre otras cosas, proporcionar un número de identificación personal (PIN) y una clave criptográfica al usuario, los cuales PIN y clave criptográfica son conocidos solamente por el usuario y la autoridad de verificación, la cual clave criptográfica comprende una pluralidad de claves de sesión y transferir un PIN codificado a una dirección predefinida de la autoridad de verificación desde el dispositivo de acceso usando un protocolo de mensajería por defecto sin utilizar capacidad de internet y sin modificar el protocolo de mensajería por defecto, que se caracteriza porque el PIN es codificado empleando una clave de sesión actual de entre la pluralidad de claves de sesión.

La sociedad solicitante respetuosamente sostiene que la invención tal como está consignada en las reivindicaciones modificadas revela una técnica de autenticación para autenticar al usuario con base en un protocolo de comunicación por defecto sin utilizar capacidad de internet, sin la instalación de ningún software de encriptación en el dispositivo de acceso, y sin modificar los protocolos de comunicación por defecto que se usan para la mensajería desde el dispositivo de acceso. Como puede apreciarse, dicha técnica puede llevarse a la práctica fácilmente en un dispositivo de acceso básico, como un teléfono móvil o dispositivo de cómputo personal descritos en las modalidades, que tengan bajas capacidades de cómputo y almacenamiento, lo cual permite asegurar las transacciones y ofrecer la inclusión financiera un gran conjunto de la población que carece de un computador o teléfono inteligente con un robusto software de encriptación con acceso a Internet y que tienen acceso limitado o nulo a cajeros automáticos.

4. D1 revela un técnica para llevar a cabo transacciones ATM/CD a través de un terminal de transacción de un banco adquirente y un banco emisor. D1 emplea técnicas estándar de encriptación/desencriptación para transferir los datos de la transacción junto con el PIN encriptado a la institución emisora desde el terminal

de transacción (p.ej., ATM o CD) de la institución adquiriente. El PIN suministrado por el usuario es encriptado con la clave de sesión. La clave de sesión de un solo uso la cual a su vez es encriptada con una clave maestra es recuperada, desencryptada usando la clave maestra, y aplicada al PIN. Esta encriptación del PIN se lleva a cabo en el terminal de transacción. Además, los datos de la transacción y el PIN encriptado se transmiten por la red del emisor para su autenticación posterior. Un código de autenticación de mensaje (MAC) se aplica a los datos transmitidos para asegurar la integridad de los datos transmitidos. Ver el Resumen de la invención en D1. No obstante, los Solicitantes respetuosamente sostienen que D1 no enseña, revela ni sugiere que el dispositivo de acceso recibe un PIN codificado proporcionado por el usuario mismo, el cual entonces es transferido a través del dispositivo de acceso a la autoridad de verificación usando un protocolo de mensajería por defecto sin utilizar la capacidad de internet y sin modificar el protocolo de mensajería por defecto de ninguna manera. Claramente, la recepción del PIN para su posterior encriptación y transmisión por la red del banco para su autenticación no es igual a la recepción de un PIN codificado para la posterior transferencia del PIN codificado usando un protocolo de mensajería por defecto sin utilizar la capacidad de internet y sin modificar el protocolo de mensajería por defecto.

D2 revela una técnica de autenticación del usuario en una red que comprende un terminal móvil, un prestador de servicio y un servidor de autenticación. El terminal móvil tiene una tarjeta inteligente con funciones de seguridad e información específica del usuario/equipo. Para beneficiarse del servicio del prestador de servicio, el usuario da información de su identidad al prestador de servicio, la cual es enviada entonces del prestador de servicio al servidor de autenticación, el cual genera un número aleatorio, el cual es enviado a la tarjeta inteligente del terminal móvil. La tarjeta inteligente crea un mensaje mediante la combinación de información específica del equipo en la tarjeta y el número aleatorio. El mensaje es firmado digitalmente por la tarjeta inteligente y luego enviado al servidor de autenticación. El servidor de autenticación desencrypta el mensaje y compara el contenido con la información del mensaje creado originalmente. El servidor de autenticación envía una confirmación al prestador de servicio si el contenido del mensaje y la mencionada información del mensaje creado originalmente se corresponden entre sí. Ver el Resumen en D2.

Claramente, esto no es igual a la invención que se reivindica y D2 no enseña, revela ni sugiere transferir un PIN codificado suministrado por el usuario a la autoridad de verificación para la autenticación posterior del usuario por la autoridad de verificación. Además, D2 no subsana las deficiencias en las enseñanzas de D1. Así las cosas, aunque se combinen, los antecedentes no enseñarían, revelarían ni sugerirían todas las características de las reivindicaciones. En particular, D1 y D2, solos o en combinación, no enseñan, revelan ni sugieren ninguna técnica de autenticación que use transferir un PIN codificado suministrado por el usuario a la autoridad de verificación usando un protocolo de mensajería por defecto sin utilizar la capacidad de internet y sin modificar el protocolo de mensajería por defecto.

5. En justicia, D1 y D2 no se pueden combinar como lo argumenta el Examinador

Además, mi representada respetuosamente sostiene que en justicia los antecedentes no se pueden combinar porque D1 y D2 no revelan ninguna técnica de autenticación en absoluto que use transferir un PIN codificado suministrado por el usuario a la autoridad de verificación usando un protocolo de mensajería por defecto sin modificar el protocolo de mensajería por defecto. *Así mismo, la persona medianamente versada en la materia técnica correspondiente no estaría motivada a modificar la técnica para llevar a cabo una transacción segura en un ATM/CD mediante la encriptación del PIN y los datos de la transacción como está descrito en D1 para emplear la técnica de autenticación del usuario de D2 porque las dos técnicas son totalmente diferentes en su naturaleza y operación y por tanto son incompatible entre sí. D1 es una procedimiento de transacción basado en la red que involucra múltiples niveles de encriptación y desencriptación para autenticar la transacción e involucra en el nivel inicial la encriptación del PIN con una clave de sesión de una sola vez almacenada en el terminal de transacción. En contraposición, D2 es un procedimiento de autenticación que involucra la generación de un número aleatorio con base en la información de identidad suministrada la cual se usa entonces para crear un mensaje mediante la combinación de información específica del equipo que está en la tarjeta y el número aleatorio. Claramente, las dos técnicas son enteramente diferentes entre sí y por lo mismo, incompatibles.*

6. El Examinador argumentó que habría sido obvio para la persona medianamente versada en la materia técnica correspondiente en el momento de la invención incluir la enseñanza de D2 en las enseñanzas de D1 por cuanto el problema técnico objetivo que pretende solucionar la presente invención podría formularse como sigue: "Cómo modificar el procedimiento de D1 para llevarlo a la práctica usando un dispositivo móvil". La sociedad solicitante asevera que el problema técnico objetivo formulado por el Examinador no es del todo correcto ya que el dispositivo móvil no puede reemplazar al terminal de transacción de la institución adquiriente como está descrito en D1 a través del cual el usuario haría su transacción con la institución emisora. *Además, incluso si uno estuviera motivado a llevar a la práctica el procedimiento de D1 usando un dispositivo móvil, simplemente pondría en efecto las técnicas reveladas en D1 en el dispositivo móvil con o sin modificaciones y no estaría tentado a diseñar un procedimiento separado completo como el revelado en D2 para llevar a cabo la autenticación o la transacción.* Así las cosas, no hay un incentivo para combinar los dos antecedentes dado que las dos técnicas son robustas y completas en sí mismas y enteramente diferentes entre sí. Claramente, entonces, D1 y D2 en combinación no revelarían transferir un PIN codificado suministrado por el usuario a la autoridad de verificación usando un protocolo de mensajería por defecto sin modificar el protocolo de mensajería por defecto. En efecto, hasta el punto en que D1 y D2 insisten en emplear mensajes encriptados generados por una máquina para llevar a cabo una transacción o para aprovechar un servicio como un procedimiento más robusto y seguro, sus enseñanzas se alejan de la invención reivindicada.

Más aún, no existe razón ni sugerencia alguna para combinar los antecedentes citados mediante la simple superposición o sustitución de la naturaleza del procedimiento de autenticación de D1 con el procedimiento de autenticación de D2 en ausencia de la presente solicitud. En tanto y cuanto D1 ya enseña una técnica de autenticación para llevar a cabo transacción segura y por ello abandona la necesidad de cualquier otra técnica de autenticación para obtener las ventajas citadas por el Examinador como motivación de la combinación, la única posible razón para la combinación sería llegar a la invención que se reivindica. Es axiomático que dar ese uso a las reivindicaciones como si fueses una hoja de ruta

es inadmisibile. No es la intención de los Solicitantes ver los antecedentes de forma individual, sino argumentar que los antecedentes no se pueden combinar, o como mínimo, que no existe motivación en el estado de la técnica para hacerlo. Cuando los antecedentes del estado de la técnica requieren una combinación seleccionada a para convertir en obvia una invención subsiguiente, tiene que haber alguna razón para la combinación diferente de la visión retrospectiva obtenida de la invención misma, es decir, algo en el estado de la técnica como un todo tiene que sugerir qué tan deseable, y por ende, qué tan obvio es hacer la combinación. No se puede usar la reconstrucción con visión retrospectiva para elegir y escoger entre las reivindicaciones aisladas del estado de la técnica para menospreciar la invención que se reivindica. Los Solicitantes respetuosamente sostienen que ninguno de los antecedentes sugiere la combinación en la que se basa el Examinador ni la motivación para dicha combinación y por tanto en justicia no se pueden combinar como lo sugiere el Examinador. De acuerdo con lo anterior, los Solicitantes creen que la combinación no es obvia para la persona medianamente versada en la materia técnica correspondiente y que el Examinador está usando una reconstrucción basada en la visión retrospectiva para elegir y escoger entre las revelaciones aisladas del estado de la técnica para menospreciar la invención que se reivindica. Más aún, los Solicitantes respetuosamente sostienen que no resulta obvio combinar la técnica de autenticación de D1 con la técnica de autenticación de D2 en tanto y cuando que estas técnicas son distintas, no están relacionadas y son incompatibles entre sí.

7. En vista de las anteriores consideraciones, mi representada sostiene que los antecedentes no establecen un caso *prima facie* obviedad de las reivindicaciones 1 y 12. Por tal razón, creemos que estas reivindicaciones y las reivindicaciones que dependen de ellas son claramente patentables con respecto a la combinación citada, y con respecto a las combinaciones de los otros antecedentes secundarios. Por ello, respetuosamente solicitamos que sean consideradas y admitidas.

Se acompaña el comprobante de pago por concepto de reivindicaciones adicionales por valor de \$ 310.000.00, recibo No. 45,102

7

Renuncio al término faltante de traslado, y les solicito otorgar el privilegio de patente de invención aquí tramitado.

De Ustedes Atentamente,

  
**LUIS FELIPE CASTILLO GIBSONE**

**T.P. No. 68.995 del C.S.J.**

**Reivindicaciones**

1. Un método para autenticar un usuario de un dispositivo de acceso por parte de una autoridad de verificación, el cual método comprende:  
proporcionar un número de identificación personal (PIN) al usuario;  
proporcionar una clave criptográfica al usuario, los cuales PIN y clave criptográfica son conocidos solamente por el usuario y la autoridad de verificación, y la cual clave criptográfica comprende una pluralidad de claves de sesión;  
transferir un PIN codificado a una dirección predefinida de la autoridad de verificación desde el dispositivo de acceso usando un protocolo de mensajería por defecto sin utilizar capacidad de internet y sin modificar el protocolo de mensajería por defecto, que se caracteriza porque el PIN es codificado empleando una clave de sesión actual de entre la pluralidad de claves de sesión y que se caracteriza porque la autoridad de verificación decodifica el PIN usando la clave criptográfica y autentica al usuario con base en una correspondencia entre el PIN decodificado y un PIN almacenado correspondiente al usuario.
2. El método de acuerdo con la reivindicación 1 que se caracteriza porque transferir el PIN codificado desde el dispositivo de acceso comprende transferir el PIN codificado desde un transceptor o un dispositivo móvil.
3. El método de acuerdo con la reivindicación 1 que se caracteriza porque el PIN comprende una secuencia de un número predefinido de caracteres.
4. El método de acuerdo con la reivindicación 1 que se caracteriza porque el PIN es codificado usando la clave criptográfica reemplazando cada carácter del PIN por un carácter correspondiente de la clave de sesión actual.
5. El método de acuerdo con la reivindicación 1 que se caracteriza porque la clave criptográfica comprende una secuencia de dígitos, que se caracteriza porque cada dígito se selecciona al azar de entre el conjunto de números (0, 1,...,9) usando un generador seguro de números aleatorios, en donde la clave criptográfica está siendo fragmentada en una pluralidad de claves de sesión que comprende 10 dígitos cada una.
6. El método de acuerdo con la reivindicación 1 que se caracteriza porque al usuario se le suministra una clave criptográfica que comprende una pluralidad de claves de sesión en la forma de un folleto de papel y que se caracteriza porque cada clave de sesión se usa para codificar el PIN solamente una vez.
7. El método de acuerdo con la reivindicación 1 que se caracteriza porque la clave criptográfica comprende una secuencia de alfabetos, que se caracteriza porque cada alfabeto se selecciona al azar de un conjunto de alfabetos predefinido usando un generador seguro de alfabetos aleatorios, en donde la clave criptográfica está siendo fragmentada en una pluralidad de claves de sesión que comprende un número predefinido de alfabetos cada una, la cual pluralidad de claves de sesión se le presenta al usuario en una pluralidad de estilos de presentación.

- 9
8. El método de acuerdo con la reivindicación 1 que se caracteriza porque la clave de sesión actual que se usa para codificar el PIN una vez es removida de la clave criptográfica por el usuario y la autoridad de verificación.
  9. El método de acuerdo con la reivindicación 1 que se caracteriza porque el PIN es almacenado por la autoridad de verificación en un formato de resumen criptográfico usando una función segura de resumen criptográfico.
  10. El método de acuerdo con la reivindicación 1 que se caracteriza porque el PIN es codificado usando la clave criptográfica reemplazando cada carácter del PIN por un carácter correspondiente de la clave de sesión actual, y que se caracteriza porque se usa un dispositivo deslizable para ayudar a buscar la clave de sesión actual, el cual dispositivo deslizable se puede desplazar sobre la pluralidad de claves de sesión permitiéndole al usuario buscar una clave de sesión deseada deslizando el dispositivo deslizable sobre un medio que contiene la clave criptográfica, el cual dispositivo deslizable comprende surcos de tamaño predefinido que hacen que cada dígito de la clave de sesión deseada caiga dentro de uno de los surcos cuando el dispositivo deslizable se pone sobre la clave de sesión deseada.
  11. Un dispositivo electrónico, que comprende:
    - una memoria que comprende una pluralidad de claves de sesión de una clave criptográfica, que se caracteriza porque cada una de entre la pluralidad de claves de sesión se usa para codificar un número de identificación personal (PIN) y que se caracteriza porque el PIN y la clave criptográfica son conocidos únicamente por un usuario y una autoridad de verificación;
    - un procesador acoplado a la memoria para recuperar una clave de sesión actual de entre la pluralidad de claves de sesión;
    - una pantalla que comprende una porción de visualización para mostrar la clave de sesión actual; y
    - por lo menos dos botones de navegación para tener acceso a una clave de sesión previa o posterior, que se caracteriza porque, para la autenticación del usuario por parte de la autoridad de verificación, el PIN es codificado empleando la clave de sesión actual y el PIN codificado es transferido a la autoridad de verificación a través de un dispositivo de acceso usando un protocolo de mensajería por defecto sin utilizar capacidad de internet y sin modificar el protocolo de mensajería por defecto.
  12. El dispositivo electrónico de acuerdo con la reivindicación 11 que se caracteriza porque el PIN comprende una secuencia de un número predefinido de caracteres.
  13. El dispositivo electrónico de acuerdo con la reivindicación 11 que se caracteriza porque el PIN es codificado reemplazando cada carácter del PIN por un carácter correspondiente de la clave de sesión actual.
  14. El dispositivo electrónico de acuerdo con la reivindicación 11 que se caracteriza porque cada clave de sesión comprende una secuencia de dígitos, que se caracteriza porque cada dígito se selecciona al azar de entre el conjunto de números (0, 1,...,9) usando un generador seguro de números aleatorios.

15. El dispositivo electrónico de acuerdo con la reivindicación 11 que se caracteriza porque la pantalla es una pantalla de LCD que comprende una primera porción de visualización para mostrar un número en clave de la sesión y una segunda porción de visualización para mostrar la clave de sesión actual.
16. El dispositivo electrónico de acuerdo con la reivindicación 11 que se caracteriza porque cada clave de sesión comprende una secuencia de alfabetos, que se caracteriza porque cada alfabeto se selecciona al azar de un conjunto de alfabetos predefinido usando un generador seguro de alfabetos aleatorios.
17. El dispositivo electrónico de acuerdo con la reivindicación 11 que se caracteriza porque el procesador le avisa al usuario que debe borrar la clave de sesión actual de la memoria una vez que la clave de sesión actual ha sido utilizada para codificar el PIN, asegurando así que una clave de sesión se usa para codificar el PIN solamente una vez.
18. El dispositivo electrónico de acuerdo con la reivindicación 11 que además comprende un transceptor para transferir el PIN codificado a la autoridad de verificación usando un protocolo de mensajería por defecto sin utilizar capacidad de internet y sin modificar el protocolo de mensajería por defecto.
19. El dispositivo electrónico de acuerdo con la reivindicación 11 que además comprende un teclado numérico para ingresar el PIN en el dispositivo electrónico, que se caracteriza porque el procesador está configurado para codificar el PIN con base en la clave de sesión actual, la pantalla está configurada para mostrar el PIN codificado, y los por lo menos dos botones de navegación están configurados para dar acceso a un PIN codificado previo o posterior.
20. Un método para autenticar un usuario de un dispositivo de acceso por parte de una autoridad de verificación, el cual método comprende:
- proporcionar un número de identificación personal (PIN) al usuario;
  - proporcionar una clave criptográfica al usuario, los cuales PIN y clave criptográfica son conocidos solamente por el usuario y la autoridad de verificación, y la cual clave criptográfica comprende una pluralidad de claves de sesión;
  - recibir un PIN codificado enviado desde el dispositivo de acceso a una dirección predefinida de la autoridad de verificación, que se caracteriza porque el PIN es codificado por el usuario o un dispositivo codificador en posesión del usuario empleando una clave de sesión actual de entre la pluralidad de claves de sesión, y que se caracteriza porque el PIN codificado es enviado desde el dispositivo de acceso usando un protocolo de mensajería por defecto sin utilizar capacidad de internet y sin modificar el protocolo de mensajería por defecto;
  - decodificar el PIN usando la clave criptográfica;
  - autenticar al usuario con base en una correspondencia entre el PIN decodificado y un PIN almacenado correspondiente al usuario.

## SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800.176.089-2

-/-

Industria y Comercio  
SUPERINTENDENCIA

## RECIBO DE CAJA

No. 14 - 0045102

Bogotá D.C., Abril 29 de 2014 - 15:13:44

RECIBIDO DE : CASTILLO GRAU &amp; ASOCIADOS LTDA.

NI 800.098.704

## \*\*\* Soporte del Pago \*\*\*

| TIPO PAGO    | BANCO           | CUENTA    | No. PAGO  | FECHA PAGO | VR. PAGO   |
|--------------|-----------------|-----------|-----------|------------|------------|
| CONSIGNACION | BANCO DE BOGOTA | 062754387 | 195869855 | 29/04/2014 | 310.000.00 |

## \*\*\* Conceptos Pagados \*\*\*

| CANT. | RENTISTICO              | CONCEPTO                                                        | Vr. UNIDITARIO | Vr. CONCEPTO |
|-------|-------------------------|-----------------------------------------------------------------|----------------|--------------|
| 10    | 50005-01-01 SOLICITUDES | 1607 REIVINDICACION PATENTE UNITARIA<br>ADICIONAL A LAS 10 INIC | 31.000.00      | 310.000.00   |
|       |                         |                                                                 |                | \$310.000.00 |

SON: \*\*TRESCIENTOS DIEZ MIL PESOS MONEDA CORRIENTE\*\*

Responsable: \_\_\_\_\_

Recibo de Caja Aplicado al Expediente No. \_\_\_\_\_

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 12-171852- -00007-0000

Fecha: 2014-04-29 15:30:54  
Tra. 11 PATENTE IYII  
Act. 523 RESPUESTADep. 2020 DIR. NUEVAS CR  
Eve: 378 FASE NACIONAL I  
Folios: 11

Sede Centro: Carrera 13 No. 27 - 00 Pisos 3,4,5 y 10 Bogotá, D.C. - Colombia

Web: www.sic.gov.co e-mail: info@sic.gov.co Conmutador: (571) 5870000 Fax: (571) 5870284 Línea: 018000-910165 Call Center: (571) 6513240

, Abril 29 de 2014 - 15:13:45