

CASTELLANOS & CO LTDA
ABOGADOS
Calle 94 A No. 7 A-09
Bogotá, D.C. – COLOMBIA

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 09-020838- -00005-0000

Fecha: 2012-06-06 14:25:43 Dep. 2020 DIR.NUEVASCR
Tra. 11 PATENTEIYII Eve: 379 FASENACIONALII
Act. 523 RESPUESTA Folios: 9

Señor

DIRECTOR DE LA DIVISIÓN DE NUEVAS CREACIONES

Superintendencia de Industria y Comercio
Ministerio de Comercio, Industria y Turismo
E. S. D.

Re.: Expediente No. **09.020.838**

Solicitud de patente PCT entrada en fase nacional para: **SISTEMA PARA
AUTORIZACION DE TRANSACCION**
Solicitante: **QPAY HOLDINGS LIMITED**

RESPUESTA AL EXAMEN DE FONDO

Yo, Margarita Castellanos Abondano, identificada como aparece al pie de mi firma, atentamente me permito presentar respuesta al oficio No. 4129 notificado por fijación en lista del 4 de marzo 2012, en los siguientes términos:

Modificaciones

En atención a las observaciones del señor examinador presento junto con este memorial un nuevo pliego de reivindicaciones en donde se corrigen los defectos de claridad y se eliminan las reivindicaciones 13 a 25 y 28 por revestir materia no patentable.

Aclaro a ese Despacho que los primeros y segundos medios de comunicación, pueden ser iguales (equivalentes) o pueden ser medios diferentes. Por ejemplo los primeros medios de comunicación pueden ser por ejemplo un teléfono (o cualquier otro dispositivo de telecomunicación) el cual llama/contacta al usuario para requerirle la autorización de la transacción. Los primeros medios de comunicación están ente el sistema de autorización y el cliente.

Los segundos medios de comunicación pueden ser Internet/e-mail o similares los cuales reciben una solicitud desde una institución para que se autorice la transacción. Los segundos medios de comunicación están entre el sistema de autorización y la institución.

En cualquier caso, los primeros y segundos medios de comunicación pueden ser iguales: en ambos casos se puede usar un teléfono, o Internet, o e-mail, o cualquier otro programa de un servidor que este designado para recibir y enviar datos de forma inalámbrica o vía Internet o línea telefónica, si embargo dichos primeros y segundos medios de comunicación pueden ser diferentes.

Habiendo aclarado cual es la función de los primeros y segundos medios de comunicación, informo que la frase "medios para" se cambió por "dispositivo para". De esta manera queda claro que dichos medios constituyen dispositivos de comunicación tales como un teléfono o cualquier otro dispositivo de telecomunicación.

Adicionalmente, se eliminaron las expresiones "por lo menos", "uno o más", etc. presentando ahora inequívocamente la materia reivindicada.

Por otra parte, en respuesta a las observaciones del señor examinador con respecto a que en las reivindicaciones se caracteriza la invención por sus usos, respetuosamente manifiesto mi desacuerdo toda vez que el sistema está bien definido por los elementos que lo componen y las frases relativas a la función que desempeña cada elemento son explicativas pues de la simple enumeración de los elementos no se desprende claramente el funcionamiento de los elementos característicos y la relación entre estos

A este respeto, el Instructivo para el Examen de Solicitudes de Patentes de Invención y Modelos de Utilidad elaborado por la SIC establece en la página 40:

"Características técnicas funcionales:

*Las características técnicas funcionales son los elementos que conforman las invenciones, descritos en términos de su uso o su función. **No definen la invención, pero explican la relación que hay entre sus diversas características estructurales.** Por ejemplo: aparato que tiene, además un "elemento para medir la presión".*

*Las reivindicaciones **deben** incluir características estructurales y funcionales cuando para la persona del oficio normalmente versada en la materia no sea obvio el funcionamiento de los elementos característicos y la relación entre estos. Por ejemplo: (Lo subrayado son características funcionales): ...*

Por otro lado, las reivindicaciones pueden incluir características estructurales y funcionales cuando para la persona del oficio normalmente versada en la materia sea obvio el funcionamiento de los elementos característicos y la relación entre estos. Por ejemplo:..” (Negrita fuera de texto)

De la lectura de éste aparte, resulta claro que la reivindicación de sistema sí debe incorporar características funcionales además de las estructurales, y que éstas no pueden interpretarse como el uso de los elementos característicos, como lo afirmó el señor examinador.

Ante la afirmación del señor examinador, relativa a que las reivindicaciones 27 y 28 no son concisas por referirse a las modalidades o dibujo del capítulo descriptivo. Llamo la atención a que dichas reivindicaciones no corresponden a las 27 y 28 sino reivindicaciones a las 24 y 25 del pliego inicial (ver publicación WO2008/014554), y que las reivindicaciones 27 y 28 del pliego reivindicatorio modificado bajo el Artículo 34 del PCT no hacen referencia a dibujos ni modalidades de la invención (ver reivindicaciones presentadas el 14 de julio de 2009 en respuesta al Oficio No. 5633 de 2009).

En conclusión, el capítulo descriptivo que presento en esta oportunidad cumple a cabalidad con los requisitos de claridad, concisión y sustento descriptivo requeridos según el artículo 30 de la Decisión 486.

Novedad

El señor examinador manifiesta que el documento D1 (US20060206709) afecta la novedad del sistema reivindicado.

Como bien lo indica el examinador, la fecha de publicación del documento D1 es 14 de septiembre de 2006, no obstante pongo de presente que dicha publicación es posterior a la fecha de prioridad de la presente invención **agosto 1, 2006**. En consecuencia no es estado del arte válido para el estudio de novedad.

No obstante, el solicitante desea informar que la publicación citada no divulga las características técnicas de ésta invención.

La presente invención proporciona un sistema que, para verificar una transacción, usa información que no está normalmente disponible para una persona fraudulenta. La solución

propuesta por esta invención recae en la combinación de las siguientes características:

- (i) el número telefónico del cliente (datos de identificación de un dispositivo de comunicación remota) se obtiene del cliente, y así mismo información de seguridad personal adicional, se requiere tener acceso al teléfono del cliente para autorizar la transacción;
- (ii) el número telefónico del cliente en (i) se guarda en un servidor/base de datos del sistema de autorización;
- (iii) los detalles de la cuenta del cliente se almacenan en un servidor/base de datos del sistema de la institución;
- (iv) dado que los detalles de (ii) y (iii) se almacenan por separado, el servidor/base de datos del sistema de autorización no conoce los detalles de la cuenta del cliente, y de igual forma el sistema de la institución no conoce el número de teléfono del cliente;
- (v) los dos diferentes sistemas de almacenamiento proporcionan una capa física de seguridad adicional para los datos del cliente, porque aún en el caso que una parte fraudulenta tenga acceso a un teléfono o número telefónico del cliente, ésta no tendría acceso a los detalles de la cuenta;
- (vi) el servidor/base de datos del sistema de autorización y el servidor/base de datos del sistema de la institución están conectados para comunicar el permiso o negación de la autorización a través de un único identificador de seguridad – el identificador no está relacionado con los detalles de la cuenta o con el número de teléfono y, en consecuencia, solamente el servidor/base de datos del sistema de autorización y el servidor/base de datos del sistema de la institución conocen esta información;
- (vii) para autorizar la transacción, en primer lugar se requiere verificar los detalles de cuenta en el sistema de la institución, luego una notificación se envía al sistema de autorización con referencia sólo al único identificador de seguridad, luego el sistema de autorización verifica al único identificador de seguridad en este sistema y envía un mensaje de verificación al cliente a través del número telefónico almacenado en la base de datos. Entonces, el cliente autoriza o niega la transacción a través de su teléfono, y el sistema de autorización transmite un mensaje con el resultado al sistema de la institución usando el único identificador de seguridad.

La solución que menciono consiste en que varias capas de seguridad y verificación de datos están almacenados **separadamente** en el sistema de autorización y en el sistema de la

institución. Así acceder a los datos almacenados en uno de los servidores no será suficiente para autorizar una transacción y en consecuencia no se podrán realizar actividades fraudulentas. Esta solución no está comprendida por el documento citado por el examinador.

La solución reclamada en la reivindicación 1 constituye una mejora en el desempeño de los sistemas computacionales existentes dado que proporciona capas de seguridad adicionales para garantizar que las transacciones se autoricen con seguridad. Los sistemas de computador existentes son más vulnerables al ataque y fraude, lo que se soluciona mediante la presente invención como se explica a continuación:

1. **Secuestro de número de telefónico** (*Phone Number Hijacking*): por ejemplo, un criminal puede robar el teléfono celular del usuario y recibir un mensaje de texto que puede ser usado para realizar una transacción fraudulenta. Una vez recibido el mensaje, el ladrón puede acceder al computador del usuario y robar del Front-end su nombre de usuario y su contraseña. Después, se roba el número telefónico y puede realizar el fraude.

En la presente invención, además del sistema de separación Back-end usando un identificador secreto -el sistema requiere de la identificación del usuario durante la llamada de autenticación- Por ejemplo, por medio de una llamada al teléfono celular del usuario, éste debe proporcionar un PIN, voz biométrica, respuesta a pregunta secreta y/o pronunciar una palabra aleatoria para identificación de voz. Esta nueva tecnología es inmune al secuestro de número telefónico y adiciona una capa de seguridad que genera mayor complejidad para los criminales. En ésta invención, el usuario necesitaría acceder al computador del usuario y robar los datos del Front-end, y **ADEMÁS** acceder a la red del teléfono celular para obtener el PIN del usuario durante una transacción, y luego robar el número de teléfono celular. Adicionalmente, en las modalidades en las que se usan identificadores biométricos de voz y una pregunta aleatoria, el criminal no puede reproducir la voz ni la respuesta utilizando la tecnología actual.

2. **Ataque man-in-the-middle** (ataque MitM): Adicionalmente, el uso de contraseña de un solo uso (One-Time-Passwords) requiere que el usuario proporcione el código de autenticación en una página online. Mediante una actividad criminal es posible la interceptación lo que se conoce como Ataque man-in-the-middle

La presente invención no emplea el canal Internet para autenticación y, por lo tanto es inmune al ataque MitM. Esto se conoce como Out-Of-Band. Este hecho refuerza la solución técnica de esta invención dado que se necesitaría el empleo simultáneo de varios servidores durante la transacción.

3. **Diversos datos de entrada:** No hay arte previo que permita el empleo de diversos datos de entrada (3 o más) a través de la capa de autenticación, como se reclama en la reivindicación 11.

En conclusión, el documento D1 no puede considerarse arte previo para el estudio de novedad y dada la explicación detallada de la solución propuesta por ésta invención, es claro que el documento D1 no proporciona las características técnicas reivindicadas y que la invención reviste novedad y altura inventiva.

Cumplido así con lo dispuesto, solicito se otorgue el privilegio de patente a la presente invención.

Anexos

- Nuevo capítulo reivindicatorio

Señor Director,


Margarita Castellanos Abondano
C.C. No. **39.779.654** de Usaquén
T.P.A. No. **70.819** de C.S.J.
Calle 94 A No. 7 A-09 – Bogotá, D.C.
Tel.: 7560770

Bogotá D.C., 6 de junio de 2012

06 JUN. 2012

REIVINDICACIONES

1. Un sistema de autorización de transacción que permite a un cliente autorizar transacciones que se relacionan con por lo menos una cuenta de cliente asociada con una institución, dicha cuenta incluye datos de identificación de cuenta almacenados en la institución, el sistema incluye:

Dispositivo de almacenamiento de datos para permitir acceso a

- (a) Datos de identificación asociados con el cliente;
- (b) Datos de identificación asociados con un dispositivo de comunicación remota (RCD) del cliente; y
- (c) Datos de identificador de seguridad que son conocidos solo por la institución y el sistema de autorización, y difieren de los datos de identificación de cuenta almacenados en la institución, los datos de identificador de seguridad que asocian una cuenta de cliente con uno o ambos de (a) y (b);

Un primer dispositivo de comunicación para permitir comunicación con el cliente por vía del RCD para autorizar una transacción sobre una cuenta de cliente; el RCD se identifica a través de la identificación de datos almacenados en el dispositivo de almacenamiento de datos;

Una arquitectura de procesamiento de datos que incluye un dispositivo de procesamiento de datos para identificar el cliente utilizando los datos de identificación (a), almacenados en el dispositivo de almacenamiento de datos, identificar el RCD utilizando los datos de identificación (b) y determinar si la transacción se autoriza por el cliente; y

Un segundo dispositivo de comunicación con la arquitectura de procesamiento de datos para recibir una petición de autorización en relación con la transacción y proporcionar una indicación a la institución de si o no la transacción se autoriza por el cliente,

en donde la petición de autorización recibida y la indicación prevista para la institución se identifican el uno al otro usando los datos de identificador de seguridad.

2. El sistema de autorización de transacción de la reivindicación 1, en donde los datos de identificador de seguridad no se comunican al cliente.
3. El sistema de autorización de transacción de la reivindicación 2, en donde el dato de identificador de seguridad no es el mismo que, ni se deriva de las características de o la información personal que se relaciona con el cliente.

4. El sistema de autorización de transacción de la reivindicación 1, en donde el primer dispositivo de comunicación permite comunicación con el cliente por vía de RCD utilizando un medio de comunicación que es distinto de los medios de comunicaciones utilizados para conducir la transacción.
5. El sistema de autorización de transacción de la reivindicación 1, en donde el primer dispositivo de comunicación permite comunicación con el cliente por vía de RCD utilizando dos o más sesiones de comunicación.
6. El sistema de autorización de transacción de la reivindicación 1, en donde (a) incluye un PIN, una clave, frase de paso y/o datos biométricos.
7. El sistema de autorización de transacción de la reivindicación 1, en donde el cliente es identificado comparando (a) con impresión de voz o un dato biométrico de voz que se deriva de una respuesta verbal del cliente a una palabra aleatoria, frase o solicitud de información proporcionada por el sistema, y comparando la respuesta verbal del cliente con una palabra aleatoriamente generada y/o información ingresada por el sistema.
8. El sistema de autorización de transacción de la reivindicación 1, en donde (b) incluye uno o más de un número telefónico, una identidad de equipo móvil internacional (IMEI), y/o dirección de protocolo de Internet (IP), y/o dirección de control de acceso de medio (MAC).
9. El sistema de autorización de transacción de la reivindicación 1, en donde el primer dispositivo de comunicación permite al cliente indicar si la transacción en por lo menos una cuenta de cliente es fraudulenta, el procesador de datos determina si el cliente ha indicado que la transacción es fraudulenta, y el segundo dispositivo de comunicación proporciona una indicación a la institución de si el cliente ha indicado como fraudulenta la transacción.
10. El sistema de autorización de transacción de la reivindicación 1, en donde el primer dispositivo de comunicación incluye un sistema de respuesta de voz interactivo (IVR).
11. El sistema de autorización de transacción de la reivindicación 10, en donde el sistema IVR provee al cliente con las opciones para autorizar la transacción, o cancelar la transacción o indicar si la transacción es fraudulenta.

12. El sistema de autorización de transacción de la reivindicación 1, en donde el dispositivo de almacenamiento de datos permite adicionalmente acceso a la información de contacto RCD para uso por el primer dispositivo de comunicación para permitir comunicación con el cliente por vía RCD.
13. Un sistema de autorización de transacción para permitir a un cliente autorizar transacciones que se relacionan con por lo menos una cuenta de cliente, el sistema incluye:

Dispositivo de almacenamiento de datos que permiten acceder a

- a) impresión de voz o datos biométricos de identificación de voz asociados con el cliente; y
- b) datos de identificación asociados con un dispositivo de comunicación remota (RCD) del cliente; y
- c) datos asociados con el cliente y/o con la cuenta del cliente;

un dispositivo de comunicación para permitir la comunicación con el cliente vía RCD y solicitar al cliente que repita verbalmente una palabra o frase generada aleatoriamente por el sistema, y/o proporciones alguna información asociada con el cliente o con la cuenta del cliente; y

Una arquitectura de procesamiento de datos que incluye procesador de datos para identificar el RCD usando (b), identificar el cliente por medio de la comparación de la palabra, frase y/o información proporcionada por el cliente con una palabra o frase generada aleatoriamente por el sistema y/o (c), y comparar la impresión de voz o dato biométrico de voz del cliente con (a), y determinar si la transacción es autorizada por el cliente;

En donde únicamente se permite al cliente autorizar una transacción una vez el cliente ha sido identificado.

14. Un sistema de pago remoto que permite a un cliente transar pagos por bienes y servicios de manera remota en una forma segura con miembros del sistema que incluye un sistema de autorización de transacción de acuerdo con una cualquiera de las reivindicaciones 1 a 14.