



Señora

Edna Marcela Ramírez Orozco

Directora de Nuevas Creaciones

Superintendencia de Industria y Comercio

E. S. D.

Referencia: Solicitud de PCT Patente de Invención denominada **SISTEMA MÓVIL PARA ACTUALIZACIÓN TRANSACCIONAL DE INFORMACIONES EN CHIPS DEL TIPO SIN CONTACTO.**

Asunto: Respuesta al Requerimiento No. 18756 de 29 de noviembre de 2021.

Expediente No. NC2018/0013079

Juan Carlos Cuesta Quintero, mayor de edad, identificado como aparece al pie de mí firma, obrando en mi calidad de apoderado de **RPC REDE PONTO CERTO TECNOLOGIA E SERVIÇOS LTDA**, doy respuesta al Oficio No. 18756 de 29 de noviembre de 2021, bajo los siguientes términos:

1. De la solicitud de patente

1.1. Reivindicaciones

El Solicitante con el objeto de dar por superadas las objeciones realizadas, ha modificado el capítulo reivindicatorio el cual ahora incluye tres reivindicaciones.

Las modificaciones realizadas tienen soporte en la descripción como se indica a continuación:

- Párrafo 1: Los dispositivos móviles tales como teléfonos inteligentes, tabletas, notebooks, relojes inteligentes.
- Párrafo 6: El método permite un proceso transaccional de actualización y autenticación de información entre un chip de tipo sin contacto y un servidor de red operativo.
- Párrafo 7: Se realiza utilizando un sistema móvil para la actualización transaccional de información.
- Párrafo 6: El sistema móvil comprende el chip tipo sin contacto y el servidor de red operativo



- Párrafo 1: Un dispositivo móvil.
- Párrafo 7: en donde el método comprende tres pasos marco de un proceso
- Párrafo 6: Transaccional de actualización y información de autenticación entre el chip de tipo sin contacto y el servidor de red operativo.
- Párrafo 7: una solicitud de usuario a través de una aplicación móvil donde: Aproximar el chip y al dispositivo móvil.
- Párrafo 6, 8, figura 1: Leer la información en ese chip por la aplicación móvil y luego procesar y cifrar la transacción solicitada por el usuario a través de una primera clave generada para garantizar la integridad de la información transaccional para la transferencia remota.
- Párrafo 7: En un segundo paso macro una autenticación en el Servidor de Red Operacional combinado con un tercer paso macro de autenticación con la clave del Emisor, comprendiendo el segundo y tercer paso.
- Figura 1: -transferir e interpretar por el servidor de la red operativa la información transaccional. El servidor operativo realiza pruebas de integridad para la información transaccional y usa una segunda clave que encripta las claves de lectura/escritura del chip propiedad de un agente de envío respectivo.
- Figura 1, párrafo 6 y 8: la segunda clave está vinculada a la respectiva transacción de solicitud de autorización de recarga. luego devolver, por parte del servidor, la respuesta transaccional a la aplicación móvil ejecutada por el dispositivo móvil del usuario; y actualizar la información en el chip, completando la operación transaccional. La segunda clave está vinculada a la respectiva transacción de solicitud de autorización de recarga.

2. Examen de patentabilidad.

2.1. Nivel inventivo

La presente invención y nueva reivindicación 1 comprende características no reveladas o sugeridas por el arte previo, como tener una primera clave cifrada que se utiliza para garantizar la integridad de la información transaccional, en la que una segunda clave cifrada vinculada a la transacción se utiliza para cifrar claves de lectura/escritura, y en la que se realiza la autenticación con una clave de emisor de un agente emisor en el servidor de la red operativa.

Adicionalmente, el solicitante no está de acuerdo con la opinión establecida por el examinador, porque los párrafos [0006] a [0008] revelan que “la figura 1 ilustra un diagrama de flujo con los pasos del proceso transaccional de actualización y autenticación de la información entre el chip de tipo sin contacto y el servidor de la red operativa” ([0006]).

Además, en el párrafo [0007], como se muestra en la Figura 1, el sistema móvil para actualización de información en chips sin contacto, objeto de esta patente de invención, consiste en un proceso



compuesto por tres macro pasos (por lo tanto, en la Fig. 1 tres cajas en una y la misma línea se muestran), a saber:

- Solicitud del usuario a través de la aplicación móvil; (-> esto se muestra en los cuadros de la izquierda y la parte de la posición del diagrama de flujo directamente debajo de los cuadros de la izquierda).
- Autenticación en el servidor de red operativo; (-> esto se muestra en los cuadros del medio y la parte de la posición del diagrama de flujo directamente debajo de los cuadros del medio.).
- Autenticación con la clave del Emisor; (-> esto se muestra en los cuadros de la derecha y la parte de la posición del diagrama de flujo directamente debajo de los cuadros de la derecha).

Por ejemplo, el párrafo [0008] establece:

- Paso 1: “El proceso transaccional se inicia con una solicitud del usuario a través del móvil aplicación para consulta o registro de información. Al acercarse al chip y al dispositivo móvil, la aplicación lee la información de ese chip y la transacción solicitada por el usuario es luego procesada y encriptada para transferencia remota. “(-> esto es se muestra en los cuadros de la izquierda y la parte de la posición del diagrama de flujo directamente debajo de la izquierda cajas.)

Los pasos 2 y 3 que se describen de forma combinada. El tercer paso comprende la solicitar autorización de recarga, que está vinculada al agente emisor que proporciona al emisor clave, también denominada 3ª clave criptográfica vinculada al número de serie del buque de la tarjeta inteligente.

El tercer paso requiere el segundo paso. Por lo tanto, los pasos 2 y 2 a descritos en una manera combinada. Aquí, el párrafo [0008] dice:

- La información transaccional luego es transferida e interpretada por el servidor operativo utilizando una segunda clave que encripta las claves de lectura/escritura del chip propiedad del respectivo agente de envío. El servidor luego devuelve la información transaccional a la aplicación ejecutado por el dispositivo móvil del usuario y actualiza la información en el chip, completando la operación transaccional.
- La interpretación comprende la Solicitud de recarga mediante la tercera clave por parte del emisor agente. La tercera clave está vinculada al número de serie del chip del carrito inteligente, según lo divulgado por Fig. 1, uno de los recuadros de la derecha.

En conclusión, la descripción puede ser corta. Sin embargo, junto con las revelaciones de la Fig. 1, las características técnicas que muestran el núcleo de la presente invención son



suficientemente revelado y respaldado por la descripción.

Así pues, la característica conocida por una persona experto en la materia no se explica ya que son conocidos por un experto en la materia. La presente solicitud se concentra una primera clave cifrada para garantizar la integridad de la información transaccional, en que se utiliza una segunda clave cifrada vinculada a la transacción para cifrar las claves de lectura/escritura, y en el que la autenticación se realiza con una clave de emisor de un agente emisor en el servidor de red, por lo que en cada etapa se utiliza una clave diferente.

Por lo tanto, se cree que las objeciones planteadas en el tema Comunicado Oficial han sido superadas completamente y la reivindicación 1 también son novedosas e implican una actividad inventiva sobre las divulgaciones del arte previo.

3. En consecuencia, le pedimos amablemente al examinador que conceda la patente para la presente invención, por lo que queda evidenciado que la invención cumple con los requisitos de patentabilidad definidos en la Decisión 486 de 2000.

Cordialmente,

Juan Carlos Cuesta Quintero.

C.C. 79.339.809 de Bogotá

T.P. 43.273 del C.S. de la J.

Anexos: Comprobante de pago por modificación voluntaria al capítulo reivindicatorio.
Capítulo reivindicatorio modificado en control de cambios.
Capítulo reivindicatorio modificado en limpio.

REIVINDICACIONES

1. Método con el fin de promover la lectura o grabación en chips utilizados entre diversos fines como medio de pago a través de dispositivos móviles tales como teléfonos inteligentes, tabletas, notebooks, relojes inteligentes, el método permite un proceso transaccional de actualización y autenticación de información entre un chip de tipo sin contacto y un servidor de red operativo y se realiza utilizando un sistema móvil para la actualización transaccional de información, el sistema móvil comprende el chip tipo sin contacto y el servidor de red operativo y un dispositivo móvil, en donde el método comprende tres pasos marco de un proceso transaccional de actualización y información de autenticación entre el chip de tipo sin contacto y el servidor de red operativo, en el que los tres pasos marco comprenden:

En un primer paso marco, una solicitud de usuario a través de una aplicación móvil donde:

- Aproximar el chip y al dispositivo móvil; y
- solicitud por parte de un usuario a través de la aplicación móvil para consulta o registro de información;
- leer la información en ese chip por la aplicación móvil y luego procesar y cifrar la transacción solicitada por el usuario a través de una primera clave generada para garantizar la integridad de la información transaccional para la transferencia remota;

En un segundo paso macro una autenticación en el Servidor de Red Operacional combinado con un tercer paso macro de autenticación con la clave del Emisor, comprendiendo el segundo y tercer paso;

-transferir e interpretar por el servidor de la red operativa la información transaccional,

- el servidor operativo realiza pruebas de integridad para la información transaccional y usa una segunda clave que encripta las claves de lectura/escritura del chip propiedad de un agente de envío respectivo, y
- la segunda clave está vinculada a la respectiva transacción de solicitud de autorización de recarga;
- realizar una autenticación con una clave de emisor que es una tercera clave de un agente emisor, la tercera clave cifrada vinculada a la transacción para cifrar claves de lectura y escritura asociadas con un número de serie de chip del chip y proporcionada por el agente emisor;
- luego devolver, por parte del servidor, la respuesta transaccional a la aplicación móvil ejecutada por el dispositivo móvil del usuario; y actualizar la información en el chip, completando la operación transaccional.

2. Método según la reivindicación 1, donde la aplicación móvil está protegida por una capa de seguridad para evitar su lectura por parte de técnicos no autorizados o posibles estafadores.

3. Método según la reivindicación 1, que comprende un modelo criptográfico para asegurar la integridad de la información transaccional transferida remotamente, reduciendo la posibilidad de fraude por inserción de un agente fraudulento entre la aplicación cliente y el servidor de comunicaciones de la red operativa.



INPI
INSTITUTO
NACIONAL
DA PROPRIEDADE
INDUSTRIAL
Assinado
Digitalmente

REPÚBLICA FEDERATIVA DO BRASIL
MINISTÉRIO DA ECONOMIA
INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL

CARTA PATENTE Nº BR 102016015611-4

O INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL concede a presente PATENTE DE INVENÇÃO, que outorga ao seu titular a propriedade da invenção caracterizada neste título, em todo o território nacional, garantindo os direitos dela decorrentes, previstos na legislação em vigor.

(21) Número do Depósito: BR 102016015611-4

(22) Data do Depósito: 04/07/2016

(43) Data da Publicação Nacional: 16/01/2018

(51) Classificação Internacional: H04W 8/24; H04W 12/04; G06Q 20/10; G06Q 20/32; G06Q 20/34; H04W 12/06.

(52) Classificação CPC: H04W 8/245; H04W 12/04; G06Q 20/105; G06Q 20/32; G06Q 20/34; H04W 12/06; H04L 63/0853.

(54) Título: SISTEMA MÓVEL PARA ATUALIZAÇÃO TRANSACIONAL DE INFORMAÇÕES EM CHIPS DO TIPO SEM CONTATO

(73) Titular: RPC REDE PONTO CERTO TECNOLOGIA E SERVIÇOS LTDA, Pessoa Jurídica. CGC/CPF: 04235110000193. Endereço: RUA REGO FREITAS, Nº 63, 2º ANDAR - CJ. 21, São Paulo, SP, BRASIL (BR), 01220-010, Brasileira

(72) Inventor: MARCELO LUIZ FERNANDES CORREA; WELLINGTON BALTAZAR DE SOUZA; AMAURI VITURINO DA SILVA JUNIOR.

Prazo de Validade: 20 (vinte) anos contados a partir de 04/07/2016, observadas as condições legais

Expedida em: 05/04/2022

Assinado digitalmente por:

Liane Elizabeth Caldeira Lage

Diretora de Patentes, Programas de Computador e Topografias de Circuitos Integrados

“SISTEMA MÓVEL PARA ATUALIZAÇÃO
TRANSACIONAL DE INFORMAÇÕES EM CHIPS DO TIPO SEM CONTATO”

Campo da Invenção

[001] A presente Patente de Invenção refere-se a um processo e respectivo sistema tecnológico empregado para o fim de promover a leitura ou gravação em chips utilizados, entre diversas finalidades, como meios de pagamento através de dispositivos móveis tais como smartphones, tablets, notebooks, smartwatches ou outros que venham a substituí-los.

Histórico da Invenção

[002] O estado da técnica contempla cartões com chip capazes de serem lidos e/ou gravados por leitores/gravadores de informação, possibilitando múltiplas aplicações tais como a criação de cartões de acesso, identificação, meios de pagamento, etc. Os chips podem ser lidos por terminais de venda permitindo a compra de produtos ou serviços sem dispor de uma conexão de dados online, como ocorre no caso de cartões de crédito ou débito. Isso possibilita a distribuição de múltiplos terminais de pontos de venda sem a necessidade de conexões físicas de dados, reduzindo significativamente o custo por manutenção de ponto de venda.

[003] Um dos principais inconvenientes presentes no estado da técnica diz respeito à dependência dos usuários com relação à rede de terminais fixos. Assim, quando um usuário encontra-se em trânsito e necessita efetuar um pagamento não dispondo eventualmente de saldo suficiente em seu cartão, ficará impossibilitado de utilizar seu chip como meio de pagamento até encontrar um terminal específico para a recarga de seus créditos.

[004] Um dos objetivos da presente Patente de Invenção reside em prover uma alternativa para que os usuários de chips do tipo sem contato realizem operações transacionais quando em trânsito, utilizando-se de um aparelho smartphone, tablet ou qualquer outro dispositivo capaz de executar aplicações móveis. Isto permitirá ao usuário total autonomia no processo de atualização ou consulta do conteúdo de seu chip, eliminando a sua dependência com relação à rede de terminais fixos.

[005] Outro objetivo da presente Patente de Invenção reside em prover uma solução segura para tráfego de dados entre o dispositivo móvel do usuário e a rede de autenticação das transações de compra, atendendo às boas práticas de segurança em criptografia de dados pela combinação de múltiplas chaves criptográficas de modo a garantir a integridade das informações e mitigar os riscos de fraude.

[006] Assim sendo, a fim de permitir a melhor elucidação do objeto em questão, proceder-se-á à sua descrição com referência à figura a seguir, onde:

a figura 1 ilustra um fluxograma com as etapas do processo transacional de atualização e autenticação de informações entre o chip do tipo sem contato e o servidor da rede operacional;

[007] De conformidade com o quanto ilustra a figura 1 acima mencionada, o sistema móvel para atualização transacional de informações em chips do tipo sem contato, objeto desta Patente de Invenção, constitui-se de um processo composto por três macro etapas, a saber:

- Solicitação do usuário via aplicação móvel;
- Autenticação no Servidor da Rede Operacional;

- Autenticação com a chave do Emissor;

[008] O processo transacional inicia com uma solicitação do usuário por meio da aplicação móvel para consulta ou gravação de informações. Aproximando-se o chip e o dispositivo móvel, as informações do referido chip são lidas pela aplicação e a transação solicitada pelo usuário é então processada e criptografada para transferência remota. A informação transacional é então transferida e interpretada pelo servidor operacional utilizando-se de uma segunda chave que criptografa as chaves de leitura/gravação do chip de propriedade do respectivo agente emissor. O servidor então devolve a informação transacional à aplicação executada pelo dispositivo móvel do usuário e atualiza a informação no chip, completando a operação transacional.

[009] Tratou-se no presente relatório descritivo de uma nova concepção para o “SISTEMA MÓVEL PARA ATUALIZAÇÃO TRANSACIONAL DE INFORMAÇÕES EM CHIPS DO TIPO SEM CONTATO”, apresentando, conforme se pode evidenciar pela descrição e pelas figuras apresentadas, algumas vantagens e aplicações diferenciadas com relação aos métodos convencionais existentes.

[010] Havendo, portanto, sido descrita e ilustrada a melhor forma de realização atualmente contemplada para a concretização da presente invenção, inúmeras modificações e variações em sua forma de realização, poderão ser prontamente introduzidas por técnicos e especialistas no assunto. No entanto, compreende-se que a presente invenção não está limitada aos aspectos práticos ilustrados e descritos no presente relatório, englobando em seu

escopo todas as variações e modificações óbvias eventualmente não descritas.

[016] Pelas vantagens que oferece e ainda por revestir-se de características técnicas verdadeiramente inovadoras, preenche todos os requisitos de originalidade e novidade no gênero, reunindo as condições necessárias para obter uma Patente de Invenção.

REIVINDICAÇÕES

1. Método para atualização transicional de informações em um chip de um dispositivo móvel usando um servidor de rede operacional, caracterizado por compreender:

receber uma solicitação de um usuário por meio de um aplicativo móvel em execução no dispositivo móvel para uma operação transacional;

ler informações do chip em resposta à solicitação do aplicativo móvel;

criptografar informações transacionais lidas do chip;

transferir as informações transacionais criptografadas remotamente para o servidor de rede operacional;

realizar uma autenticação no servidor de rede operacional;

realizar uma autenticação com uma primeira chave do emissor: e atualizar as informações no chip com base em uma resposta transacional do servidor de rede operacional;

em que o aplicativo móvel é composto por um código fonte protegido por uma camada de segurança para evitar a leitura por terceiros não autorizados.

2. Método, de acordo com a reivindicação **1**, caracterizado por adicionalmente compreender usar múltiplas chaves criptográficas juntamente com as etapas de autenticação.

3. Método, de acordo com a reivindicação **2**, caracterizado por adicionalmente compreender assegurar a

integridade das informações transacionais transferidas remotamente com um modelo criptográfico, reduzindo a possibilidade de fraude.

4. Método, de acordo com a reivindicação **2**, caracterizado por adicionalmente compreender usar uma segunda chave que criptografa chaves de leitura e gravação associadas a um número de série do chip.

5. Método, de acordo com a reivindicação **3**, caracterizado por o modelo criptográfico reduzir a possibilidade de fraude pela inserção de um agente fraudulento entre o aplicativo móvel e o servidor da rede operacional.

6. Método, de acordo com a reivindicação **4**, caracterizado por as informações transacionais serem transferidas e interpretadas pelo servidor de rede operacional usando a segunda chave; e em que o número de série é fornecido por um agente de envio.

7. Método para atualização transicional de informações em um chip de um dispositivo móvel usando um servidor de rede operacional, caracterizado por compreender: receber uma solicitação de um usuário por meio de um aplicativo móvel em execução no dispositivo móvel para uma operação transacional;

ler informações do chip em resposta à solicitação do aplicativo móvel; gerar uma primeira chave criptografada para assegurar a integridade das informações transacionais lidas do chip;

criptografar as informações transacionais para transferência remota;

transferir as informações transacionais criptografadas remotamente para o servidor de rede operacional;

pelo servidor de rede operacional, testar a integridade das informações transacionais;

pelo servidor de rede operacional, realizar uma autenticação com uma chave do emissor de um agente emissor;

pelo servidor de rede operacional, usar uma segunda chave criptografada associada à transação para criptografar chaves de leitura e gravação associadas a um número de série de chip do chip e fornecida pelo agente emissor;

pelo servidor de rede operacional, determinar uma resposta transacional;

retornar a resposta transacional para o aplicativo móvel em execução no dispositivo móvel pelo servidor de rede operacional; e

atualizar as informações no chip com base na resposta transacional do servidor de rede operacional;

em que o aplicativo móvel compreende um código fonte protegido por uma camada de segurança para evitar a leitura por técnicos não autorizados ou potenciais fraudadores.

8. Método, de acordo com a reivindicação 7, caracterizado por teste de integridade para as informações transacionais compreender o uso de um modelo criptográfico, reduzindo a possibilidade de fraude pela inserção de um agente fraudulento entre o aplicativo móvel e o servidor de rede operacional.

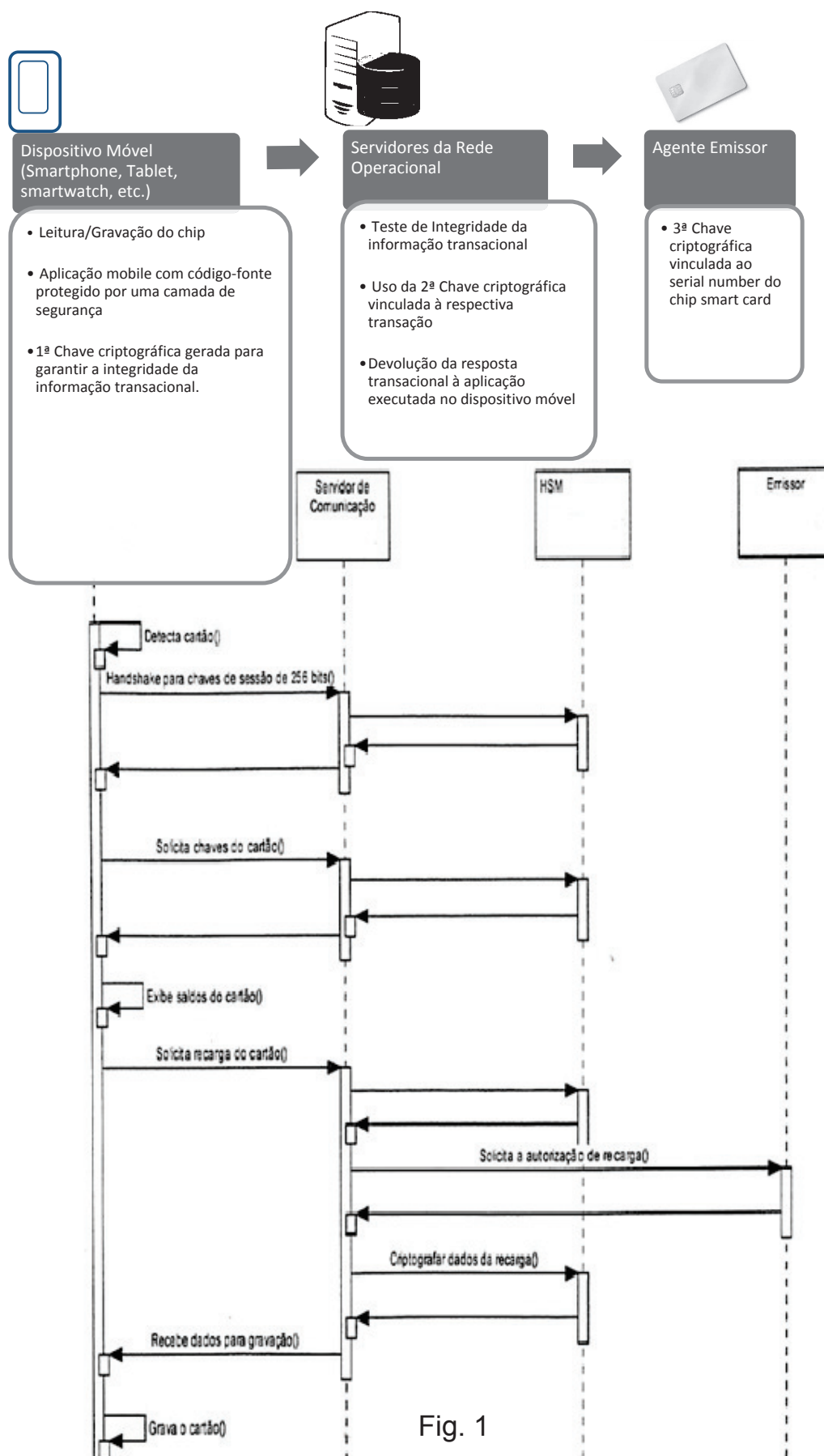


Fig. 1



Letter accompanying subsequently filed items

Representative:

Ferdinand Stöckeler
SCHOPPE, ZIMMERMANN, STÖCKELER, ZINKLER, SCHENK &
Partner mbB
Radlkoferstr. 2
81373 München
Germany

Phone: 089-790 445-0
Fax: 089-790 22 15
E-mail: mail@schoppe-zimmermann.com

80298 Munich
Germany
Tel. +49(0)89 2399-0 | Fax -4465

P.O. Box 5818
2280 HV Rijswijk
Netherlands
Tel. +31(0)70 340-2040 | Fax -3016

10958 Berlin
Germany
Tel. +49(0)30 25901-0 | Fax -840

The document(s) listed below is (are) subsequently filed documents pertaining to the following application:

Application number

17823354.0

Applicant's or representative's reference

RPC170601PEP

	Description of document	Original file name	Assigned file name
1	Reply to examination report	Reply.pdf	EXRE3-1.pdf
2	Amended claims (clean copy)	Claims - Main Request_clean version.pdf	CLMS-1.pdf
3	Amended claims with annotations	Claims - Main Request_marked-up version.pdf	CLMS-HWA-1.pdf
4	Amended claims (clean copy)	Claims - Auxiliary Request_clean version.pdf	CLMS-2.pdf
5	Amended claims with annotations	Claims - Auxiliary Request_marked-up version.pdf	CLMS-HWA-2.pdf

	Payment	
1	Method of payment	Not specified

Signatures

Place: **München**
Date: **08 March 2022**
Signed by: **Ferdinand Stöckeler 9620**
Representative name: **Ferdinand Stöckeler**
Capacity: **(Representative)**

RPC170601PEP

Patentanwälte ■ Radlkoferstraße 2 ■ 81373 München

European Patent Office

80298 Munich

Tankred Zimmermann ■ Dipl.-Ing.

Ferdinand Stöckeler ■ Dipl.-Ing.

Franz Zinkler ■ Dipl.-Ing.

Markus Schenk ■ Dipl.-Phys.

Günter Hersina ■ Dipl.-Ing.

Markus Burger ■ Dipl.-Ing.

Oliver Schairer ■ Dipl.-Inf. Univ.^Δ

Julian Schlenker ■ Dipl.-Ing.^Δ

Hannes Pfitzner ■ Dipl.-Ing.^Δ

Andreas König ■ Dipl.-Ing. M.Sc.^Δ

March 8, 2022

European Patent Application 17823354.0

Applicant: RPC REDE PONTO CERTO TECNOLOGIA E SERVIÇOS LTDA

**Title: PORTABLE SYSTEM FOR UPDATING TRANSACTION INFORMATION ON
CONTACTLESS CHIPS**

Our reference: RPC170601PEP / ex / ai / sc

In reply to the Official Communication pursuant Article 94(3) EPC dated October 14, 2021:

I. Requests

The issuance of the Official Communication pursuant to Rule 71(3) EPC is respectfully requested for the following application documents:

Claims, Numbers

1-3 as enclosed in the main request, or

1-3 as enclosed in the auxiliary request,

Description, Paragraphs

1-11 as published

Drawings, Sheets

1/1 as published

In case of any further objections, issuance of another Official Communication pursuant to Article 94(3) EPC is respectfully requested. As an auxiliary measure, it is respectfully requested to schedule a date for a personal interview or for Oral Proceedings pursuant to Article 116 EPC.

II. Remarks

With regard to the first communication pursuant to Article 94(3) EPC, the applicant disagrees with the Examining Division's opinion that the amended claims filed with letter of September 14, 2021 cannot be considered to comply with the requirements of the EPC, in particular in view of Articles 123(2), 83 and 84 EPC.

With regard to issue 4.4 of said communication, the applicant disagrees with the Divisions opinion as will be further explained below.

The Division states that only par. [0007] and [0008] of the description are the only two paras. of the description containing any information of substance in relation with what could be called an embodiments of the invention.

With this opinion the applicant disagrees, because the paragraphs [0001] and [0006] should additionally considered.

With regard to the other two sources (i.e. text boxes and flow scheme of Fig. 1), the division is of the opinion that the three sources do not have any clear and unambiguous relation to each other.

The applicant disagrees this opinion, as will be further explained below.

The amended claims of the auxiliary enclosed are amended based on the disclosure of the description and the text boxed of Fig. 1. The relation will be explained in detail below.

III. Amendments

Main request

The claim 1 of the main request, that is based on the claims filed with letter of September 14, 2021, is amended by deleting from the term "a chip ~~of a mobile device~~" the strikethrough part.

Auxiliary request

A new claim 1 is drafted using the literal disclosure of the description and the Fig. 1.

The Examiner is requested to view the enclosed marked-up versions of the claims for details.

IV. Added subject-matter according to Article 123(2) EPC and clarity and Sufficiency of disclosures according to Articles 83 and 84 EPC

The issue under 4.1 of the Office Action is believed to be overcome in view of the amendments made to claim 1 of the main request.

The applicant disagrees with the opinion set out under issue 4.2 of the Office action, because the paragraphs [0006] to [0008] disclose that "figure 1 illustrates a flow chart with the steps of the transactional process of updating and authenticating information between the contactless type chip and the operational network server" ([0006]).

Further: [0007] Accordingly as shown in Figure 1 above, the mobile system for transitional updating of information in contactless chips, object of this patent of invention, consists of a process composed of **three** macro steps (therefore in Fig. 1 three boxes in one and the same line are shown), namely:

User request via mobile application; (-> this is shown in the left boxes and the part of the flow chart position directly below the left boxes.)

Authentication on Operational Network Server; (-> this is shown in the middle boxes and the part of the flow chart position directly below the middle boxes.)

Authentication with the Issuer key; (-> this is shown in the right boxes and the part of the flow chart position directly below the right boxes.)

The paragraph [0008] reads:

1 step: "The transactional process starts with a request from the user through the mobile application for query or information recording. Approaching the chip and the mobile

device, the information on that chip is read by the application and the transaction requested by the user is then processed and encrypted for remote transfer. “(-> this is shown in the left boxes and the part of the flow chart position directly below the left boxes.)

The 2. and 3 steps are disclosed in a combined fashion. The third step comprises the request authorization to recharge, which is linked to the issuing agent providing the issuer key, also called 3rd cryptographic key linked to the serial number of the smart card chip. The third step requires the second step. Therefore, step 2 and 2 a described in a combined manner. Here, the paragraph [0008] reads:

“The transactional information is then transferred and interpreted by the operational server using a second key that encrypts the chip read/write keys owned by the respective sending agent. The server then returns the transactional information to the application executed by the user's mobile device and updates the information on the chip, completing the transactional operation.

The interpretation comprises the Request to recharge using the third key by the issuing agent. The third key is linked to the serial number of the smart card chip, as disclosed by Fig. 1, one of the right boxes.

In conclusion, the description may be short. However, in conjunction with the disclosures of Fig. 1, the technical features showing the core of the present invention are sufficiently disclosed and supported by the description. Stated differently, the spice is in the brevity.

As already explained in the letter of September 14, 2021, the feature known to a person skilled in the art are not explained since they are known by a person skilled in the art. It was not considered necessary then time when drafting this application that features known to a person skilled in the art needs to be described in detail. The present application concentrates on the features being part of the present invention.

That is a first encrypted key is used to ensure the integrity of transactional information, in which a second encrypted key linked to the transaction is used to encrypt read/write keys, and in which authentication is performed with an issuer key of an issuing agent at the operational network server. Thus, at each stage a different key is used.

V. Novelty and inventive step

Main request

The European search opinion refers to D1 (US7729986B1) as far as patentability of the claimed subject matter is concerned. It is, however, not foreseeable where D1 shows an approach as defined in the newly submitted independent claim, in which a first encrypted key is used to ensure the integrity of transactional information, in which a second encrypted key linked to the transaction is used to encrypt read/write keys, and in which authentication is performed with an issuer key of an issuing agent at the operational network server. Thus, it is believed that D1 does prejudice patentability of the newly submitted claims.

Auxiliary request

The claim 1 of the auxiliary request is newly drafted, because the Examiner states under issue 4.3, that an exhaustive list of all issues arising from the amendments made to the feature of the claims of the main request would exist.

From the above, the applicant's point of view is provided explaining why the applicant believes that the present invention is well disclosed and supported by the description and the Fig. 1.

Unfortunately, the Applicant does not get any chance to get to know about the exhaustive list of all issues, because the Examiner thinks there is not even a remote chance to overcome these issues.

That is why, a new claim 1 using the literal disclosures of the description and of Fig. 1 is enclosed as an auxiliary request.

As already explained above, also the claim 1 of the auxiliary request comprises the features not disclosed or suggested by D1. That is a first encrypted key is used to ensure the integrity of transactional information, in which a second encrypted key linked to the transaction is used to encrypt read/write keys, and in which authentication is performed with an issuer key of an issuing agent at the operational network server.

It is respectfully requested to postpone any revision of the specification until an allowable claim version has been established.

VI. Conclusions

It is believed that the objections raised in the subject Official Communication have been dealt with completely and it could be shown that the claims 1 of the main and the auxiliary requests are also novel and involve an inventive step over the disclosures of D1 and fulfill the requirements of Articles 83, 84 and 123(2) EPC. Thus, issuance of the Official Communication pursuant to Rule 71(3) EPC is respectfully requested.

Respectfully submitted,

Ferdinand Stöckeler

Enclosures

Amended claims of a main request (marked-up and clean copy)

Amended claims of an auxiliary request (marked-up and clean copy)

Main request

CLAIMS

1. Method for transitional updating of information in a chip using an operational network server, the method allowing a chip user to perform a transactional operation when in transit, using a mobile device, such as a smartphone, tablet, notebook, smartwatch or any other device capable of running mobile applications, the method comprising:

upon a request by the user through a mobile application running on the mobile device for a transactional operation, such as a query or information recording, reading information on the chip, generating a first encrypted key to ensure the integrity of transactional information and encrypting the transactional information for remote transfer,

transferring the encrypted transactional information to an operational network server,

by the operational network server, integrity testing for the transactional information, performing an authentication with an issuer key of an issuing agent, using a second encrypted key linked to the transaction to encrypt read and write keys associated with a chip serial number of the chip and provided by the issuing agent and returning a transactional response to the application running on the mobile device, and

updating information on the chip to complete the transactional operation.

2. Method according to claim 1, wherein the mobile application is composed of a source code protected by a security layer to avoid reading by unauthorized technicians or potential fraudsters.

3. Method according to claim 1, comprising a cryptographic model for ensuring the integrity of the transactional information transferred remotely, reducing the possibility of fraud by insertion of a fraudulent agent between the client application and the communication server of the operational network.

Main requestCLAIMS

1. Method for transitional updating of information in a chip ~~of a mobile device~~ using an operational network server, the method allowing a chip user to perform a transactional operation when in transit, using ~~a~~the mobile device, such as a smartphone, tablet, notebook, smartwatch or any other device capable of running mobile applications, the method comprising:

upon a request by the user through a mobile application running on the mobile device for a transactional operation, such as a query or information recording, reading information on the chip, generating a first encrypted key to ensure the integrity of transactional information and encrypting the transactional information for remote transfer,

transferring the encrypted transactional information to an operational network server,

by the operational network server, integrity testing for the transactional information, performing an authentication with an issuer key of an issuing agent, using a second encrypted key linked to the transaction to encrypt read and write keys associated with a chip serial number of the chip and provided by the issuing agent and returning a transactional response to the application running on the mobile device, and

updating information on the chip to complete the transactional operation.

2. Method according to claim 1, wherein the mobile application is composed of a source code protected by a security layer to avoid reading by unauthorized technicians or potential fraudsters.

3. Method according to claim 1, comprising a cryptographic model for ensuring the integrity of the transactional information transferred remotely, reducing the possibility of fraud by insertion of a fraudulent agent between the client application and the communication server of the operational network.

Auxiliary request

CLAIM

1. Method for the purpose of promoting reading or recording on chips used among various purposes as means of payment through mobile devices such as smartphones, tablets, notebooks, smartwatches, the method allows a transactional process of updating and authenticating information between a contactless type chip and an operational network server and is performed using a mobile system for transitional updating of information, the mobile system comprises the contactless type chip and the operational network server and a mobile device, wherein the method comprises three macro steps of a transactional process of updating and authenticating information between the contactless type chip and the operational network server, wherein the three macro steps comprises:

In a first macro step a user request via a mobile application comprising

- at first approaching the chip and the mobile device; and
- requesting by a user through the mobile application for query or information recording;
- reading the information on that chip by the mobile application and the transaction requested by the user is then processed and encrypted via a first key generated to ensure the integrity of transactional information for remote transfer;

In a second macro step an authentication on Operational Network Server combined with a third macro step of authentication with the Issuer key, the second and third steps comprising;

- transferring to and interpreting by the operational network server then the transactional information,
- the operational server performing integrity testing for the transactional information and using a second key that encrypts the chip read/write keys owned by a respective sending agent, and
- the second key is linked to the respective transaction of requesting authorization to recharge;

- performing an authentication with an issuer key being a third key of an issuing agent, the third encrypted key linked to the transaction to encrypt read and write keys associated with a chip serial number of the chip and provided by the issuing agent;

- then returning, by the server, the transactional response to the mobile application executed by the user's the mobile device; and

- updating the information on the chip, completing the transactional operation.

2. Method according to claim 1, wherein the mobile application is composed of a source code protected by a security layer to avoid reading by unauthorized technicians or potential fraudsters.

3. Method according to claim 1, comprising a cryptographic model for ensuring the integrity of the transactional information transferred remotely, reducing the possibility of fraud by insertion of a fraudulent agent between the client application and the communication server of the operational network.

Auxiliary request

CLAIM

1. Method for the purpose of promoting reading or recording on chips used among various purposes as means of payment through mobile devices such as smartphones, tablets, notebooks, smartwatches **{paragraph [0001] of the description}**, the method allows a transactional process of updating and authenticating information between a contactless type chip and an operational network server [0006] and is performed using a mobile system for transitional updating of information **{paragraph [0007] of the description}**, the mobile system comprises the contactless type chip and the operational network server [0006] and a mobile device [0001], wherein the method comprises three macro steps [0007] of a transactional process of updating and authenticating information between the contactless type chip and the operational network server [0006], wherein the three macro steps comprises: **{see[0007] and [0008]}**

In a first macro step a user request via a mobile application comprising [0007]

-at first **(instead of start with, see [0007])** approaching the chip and the mobile device; and

- requesting by a user through the mobile application for query or information recording;

- reading the information on that chip by the mobile application and the transaction requested by the user is then processed and encrypted via a first key generated to ensure the integrity of transactional information for remote transfer; **{Fig.1 (left box) in conjunction with [0008] and [0006] stating that Fig. 1 illustrates a flow chart with the steps... }**

In a second macro step an authentication on Operational Network Server combined with a third macro step of authentication with the Issuer key, the second and third steps comprising [0007]

-transferring to and interpreting by the operational network server (**Fig. 1 the flow from the left to the middle box and the right box**) then the transactional information,

- the operational server performing integrity testing for the transactional information (**Fig. 1 middle box**) and using a second key that encrypts the chip read/write keys owned by a respective sending agent, (**Fig. 1, middle box**) and

- the second key is linked to the respective transaction of requesting authorization to recharge; **Fig.1 (middle and right box) in conjunction with [0008] and [0006] stating that Fig. 1 illustrates a flow chart with the steps..., and in conjunction with the flow chart, see from middle col. to right col.}**

-performing an authentication with an issuer key being a third key of an issuing agent, the third encrypted key linked to the transaction to encrypt read and write keys associated with a chip serial number of the chip and provided by the issuing agent(**Fig. 1, right box**);

-then returning, by the server, the transactional response to the mobile application executed by the user's the mobile device; **Fig.1 (middle box) in conjunction with [0008] and [0006] stating that Fig. 1 illustrates a flow chart with the steps... }**; and updating the information on the chip, completing the transactional operation **[0008]**.

2. Method according to claim 1, wherein the mobile application is composed of a source code protected by a security layer to avoid reading by unauthorized technicians or potential fraudsters.

3. Method according to claim 1, comprising a cryptographic model for ensuring the integrity of the transactional information transferred remotely, reducing the possibility of fraud by insertion of a fraudulent agent between the client application and the communication server of the operational network.



**SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA ECONOMIA
INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL**

RELATÓRIO DE BUSCA

N.º do Pedido: BR102016015611-4 **N.º de Depósito PCT:**
Data de Depósito: 04/07/2016
Prioridade Unionista: -
Depositante: RPC REDE PONTO CERTO TECNOLOGIA E SERVIÇOS LTDA (BRSP)
Inventor: MARCELO LUIZ FERNANDES CORREA, WELLINGTON BALTAZAR DE SOUZA, AMAURI VITURINO DA SILVA JUNIOR
Título: "Sistema móvel para atualização transacional de informações em chips do tipo sem contato"

1 - CLASSIFICAÇÃO **IPC** H04W 8/24, H04W 12/04, G06Q 20/10, G06Q 20/32,
G06Q 20/34, H04W 12/06

CPC

2 - FERRAMENTAS DE BUSCA

☐ EPOQUE	☒ ESPACENET	☐ PATENTSCOPE	☒ Derwent
☐ DIALOG	☐ USPTO	☐ SINPI	
☐ CAPES	☐ SITE DO INPI	☐ STN	

3 - REFERÊNCIAS PATENTÁRIAS

Número	Tipo	Data de publicação	Relevância *
US7729986	B1	01/06/2010	A
US20040127256	A1	01/07/2004	A

4 - REFERÊNCIAS NÃO-PATENTÁRIAS

Autor/Publicação	Data de publicação	Relevância *

Observações:

Rio de Janeiro, 22 de fevereiro de 2022.

Paulo Roberto Dutra Magalhaes
Pesquisador/ Mat. Nº 1287310
DIRPA / CGPAT III/DICEL
Deleg. Comp. - Port. INPI/DIRPA Nº
008/13

* Relevância dos documentos citados:

- A documento que define o estado geral da técnica, mas não é considerado de particular relevância;
- N documento de particular relevância; a invenção reivindicada não pode ser considerada nova quando o documento é considerado isoladamente;
- I documento de particular relevância; a invenção reivindicada não pode ser considerada dotada de atividade inventiva ou de ato inventivo quando o documento é considerado isoladamente;

Y documento de particular relevância; a invenção reivindicada não pode ser considerada dotada de atividade inventiva quando o documento é combinado com um outro documento ou mais de um;

PN documento patentário, publicado após a data de depósito do pedido em exame, ou da prioridade requerida para o pedido em exame, cuja data de depósito, ou da prioridade reivindicada, é anterior a data de depósito do pedido em exame, ou da prioridade requerida para o pedido em exame; esse documento patentário pertence ao estado da técnica para fins de novidade, se houver correspondente BR, conforme o Art. 11 §2.º e §3.º da LPI.



**SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA ECONOMIA
INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL**

RELATÓRIO DE EXAME TÉCNICO

N.º do Pedido: BR102016015611-4 **N.º de Depósito PCT:**
Data de Depósito: 04/07/2016
Prioridade Unionista: -
Depositante: RPC REDE PONTO CERTO TECNOLOGIA E SERVIÇOS LTDA (BRSP)
Inventor: MARCELO LUIZ FERNANDES CORREA, WELLINGTON BALTAZAR DE SOUZA, AMAURI VITURINO DA SILVA JUNIOR
Título: "Sistema móvel para atualização transacional de informações em chips do tipo sem contato "

PARECER

O presente pedido refere-se a uma alternativa para que os usuários de chips do tipo sem contato realizem operações transacionais quando em trânsito, utilizando-se de um aparelho smartphone, tablet ou qualquer outro dispositivo capaz de executar aplicações móveis. Isto permitirá ao usuário total autonomia no processo de atualização ou consulta do conteúdo de seu chip, eliminando a sua dependência com relação à rede de terminais fixos.

Admitido o trâmite prioritário requerido através da petição nº 870210099220, de 27/10/2021, haja vista que atende ao disposto nos artigos 3º e 4º da Portaria INPI PR nº 404, de 21/12/2020, publicada na RPI 2654, de 16/11/2021.

Quadro 1 – Páginas do pedido examinadas

Elemento	Páginas	n.º da Petição	Data
Relatório Descritivo	4 Págs. (Págs. 13 a 16 do PDF)	870160033471	04/07/2016
Quadro Reivindicatório	3 Págs. (Págs. 20 a 22 do PDF)	870210099220	27/10/2021
Desenhos	1 Pág. (Pág. 20 do PDF)	870160033471	04/07/2016
Resumo	1 Pág. (Pág. 19 do PDF)	870160033471	04/07/2016

Quadro 2 – Considerações referentes aos Artigos 10, 18, 22 e 32 da Lei n.º 9.279 de 14 de maio de 1996 – LPI

Artigos da LPI	Sim	Não
A matéria enquadra-se no art. 10 da LPI (não se considera invenção)		X
A matéria enquadra-se no art. 18 da LPI (não é patenteável)		X
O pedido apresenta Unidade de Invenção (art. 22 da LPI)	X	
O pedido está de acordo com disposto no art. 32 da LPI	X	

Comentários/Justificativas

Quadro 3 – Considerações referentes aos Artigos 24 e 25 da LPI		
Artigos da LPI	Sim	Não
O relatório descritivo está de acordo com disposto no art. 24 da LPI	X	
O quadro reivindicatório está de acordo com disposto no art. 25 da LPI	X	

Comentários/Justificativas

Quadro 4 – Documentos citados no parecer		
Código	Documento	Data de publicação
D1	US7729986	01/06/2010
D2	US20040127256	01/07/2004

Quadro 5 – Análise dos Requisitos de Patenteabilidade (Arts. 8.º, 11, 13 e 15 da LPI)		
Requisito de Patenteabilidade	Cumprimento	Reivindicações
Aplicação Industrial	Sim	1 a 8
	Não	-
Novidade	Sim	1 a 8
	Não	-
Atividade Inventiva	Sim	1 a 8
	Não	-

Comentários/Justificativas: o pedido possui atividade inventiva.

Conclusão

A matéria reivindicada apresenta novidade, atividade inventiva e aplicação industrial (Art. 8º da LPI), e o pedido está de acordo com a legislação vigente, encontrando-se em condições de obter a patente pleiteada.

Assim sendo, defiro o presente pedido como Patente de Invenção, devendo integrar a Carta Patente **os documentos que constam no Quadro 1 deste parecer, exceto o resumo.**

Para a concessão da patente o depositante deverá efetuar o pagamento da retribuição e a respectiva comprovação correspondente à expedição da carta-patente, conforme os prazos estabelecidos no Artigo 38 da LPI.

Publique-se o deferimento (9.1).

Rio de Janeiro, 22 de fevereiro de 2022.

Paulo Roberto Dutra Magalhaes
Pesquisador/ Mat. Nº 1287310
DIRPA / CGPAT III/DICEL
Deleg. Comp. - Port. INPI/DIRPA Nº
008/13



SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT: 800.176.089-2

COMPROBANTE DE RECAUDO SISTEMA SIPI

Radicado: NC2018/0013079

Recibo: 22-30292

Fecha: 08/04/2022

JUAN CARLOS CUESTA QUINTERO

CC: 79.339.809

Pago PSE No: 659285

CUS: 1406242210

Patente PCT

SISTEMA MÓVIL PARA ACTUALIZACIÓN TRANSACCIONAL DE INFORMACIONES EN CHIPS DEL TIPO SIN CONTACTO

Detalle del pago

Id.	Rentístico	Concepto y Servicio	Cant.	Val. Unit.	Subtotal
1	50005-01-03	Modificaciones / Correcciones al registro Patente PCT (DESCUENTO INTERNET)	1	\$ 176,000	\$ 176,000
TOTAL					\$ 176,000