

SOLICITUD

PATENTE DE INVENCION

11-82169

21. EXPEDIENTE No.

54. TÍTULO **"MÉTODO Y SISTEMA PARA PROCESAR DE MANERA SEGURA UNA TRANSACCIÓN".**

51. CLASIFICACIÓN INTERNACIONAL **G06Q 20/00**

71. SOLICITANTE **MTN MOBILE MONEY SA (PTY) LTD**

DOMICILIO **FAIRLANDS, SUDAFRICA**

74. REPRESENTANTE LEGAL **ALICIA LLOREDA RICAURTE**
T.P. 53.215

30 JUN 2011

22. BOGOTÁ, D.C.

(FORMA P 10)

PETITORIO



SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 11-082169- -00000-0000

Fecha: 2011-06-30 16:57:06 Dep. 2020 DIR.NUEVASCR
Tra. 11 PATENTEIYII Eve: 378 FASENACIONALI
Act. 411 PRESENTACION Folios: 49

FORMULARIO ÚNICO DE SOLICITUD DE PATENTE PCT ENTRADA EN FASE NACIONAL

①

SOLICITUD DE:

☒ Patente de Invención

☐ Patente de Modelo de Utilidad

☒ Capítulo I.

☐ Capítulo II.

②

SOLICITANTE (71)

Nombre: **MTN MOBILE MONEY SA (PTY) LTD**

Dirección: 216 14th Avenue, 2022 Fairlands, Sudáfrica.

Nacionalidad o Domicilio: Fairlands, Sudáfrica.

Lugar de Constitución:

Teléfono: 3264270 Fax: 6069701

E-mail: jllcco@lloredacamacho.com

IDENTIFICACION

C.C. ☐ NIT ☐
C.E. ☐ Otro ☐

Cual _____

Número _____

③

REPRESENTANTE O APODERADO

Nombre: **ALICIA LLOREDA RICAURTE**

Dirección: Calle 72 No. 5-83 Piso 5º, Bogotá, Colombia

Teléfono: 3264270 Fax: 6069701

E-mail: jllcco@lloredacamacho.com

C.C. ☒ NIT ☐
C.E. ☐ Otro ☐

Cual _____

Número 39.690.713 TP 53.215

④

INVENTOR(ES) (72)

Nombre: **BRUYNSE, Dirk, Marinus y BEZUIDENHOUDT, Schalk, Johann.**

Dirección: 43 Dianne Road, Olivedale, 2158 Johannesburg y 5 Cliffside Crescent, 2115 Northcliff.

Nacionalidad o Domicilio: Sudáfrica.

⑤

PCT (86)

Solicitud Internacional No. PCT/IB2009/055838

Fecha: 18/12/09

Publicación Internacional No. WO 2010/073199 A1

Fecha: 01/07/10

⑥

Título (54)

"MÉTODO Y SISTEMA PARA PROCESAR DE MANERA SEGURA UNA TRANSACCIÓN"

⑦

Clasificación Internacional (51) G06Q 20/00

⑧

Prioridad

SI ☒ NO ☐

(33) País de Origen

ZA

(32) Fecha

23/12/08

(31) Número de Solicitud

2008/10835

⑨

Comprobante de Pago No. 11-0052109

Fecha: 31 de Mayo de 2011

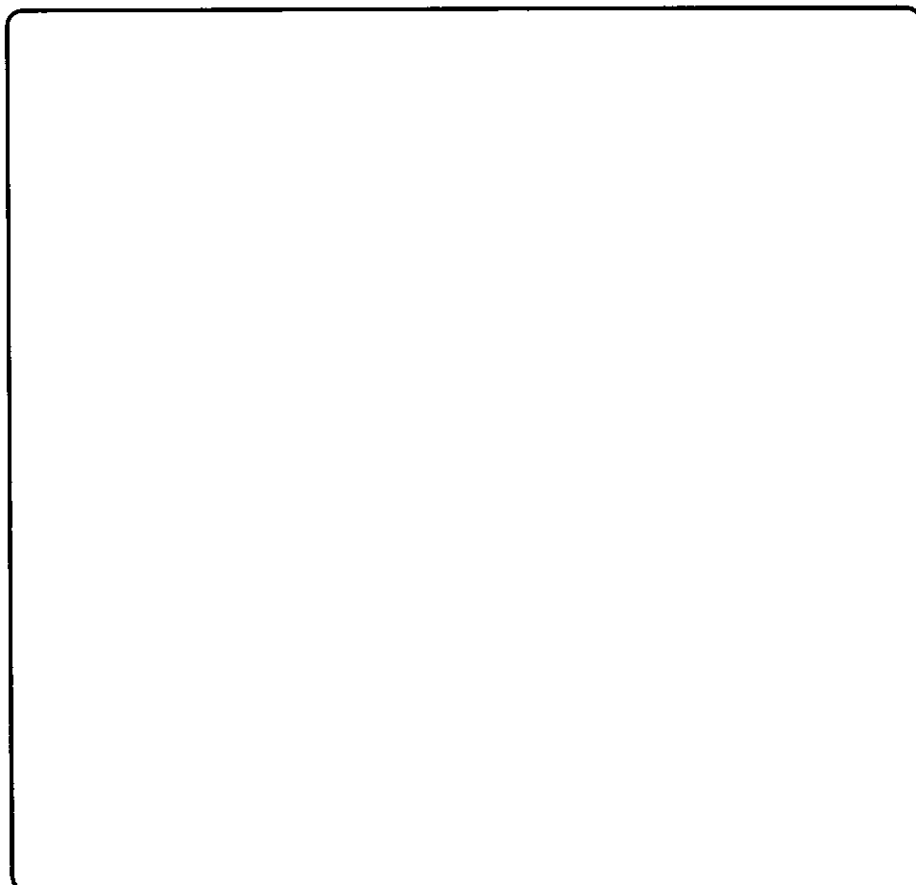
10

ANEXOS

- ☒ Comprobante de pago de la tasa de presentación de la solicitud.
- ☐ Documento que acredita la existencia y representación legal cuando el solicitante sea persona jurídica.
- ☐ Documento de Representación Legal.
- ☐ Documento de cesión del inventor al solicitante o a su causante.
- ☐ Declaraciones.
- ☐ Copia de la solicitud internacional. (Resumen, descripción, reivindicaciones, dibujos)
- ☒ Traducción de la solicitud internacional al castellano. (Resumen, descripción, reivindicaciones y dibujos)
- ☐ Copia del reporte preliminar internacional sobre patentabilidad.
- ☐ Traducción del reporte preliminar internacional sobre patentabilidad.
- ☐ De ser el caso, copia del contrato de acceso.
- ☐ De ser el caso, documento que acredite la licencia o autorización de uso de conocimientos tradicionales de las comunidades indígenas.
- ☐ Arte Final 12X12.
- ☐ De ser el caso, información sobre otras solicitudes de patente o títulos obtenidos en el extranjero por el mismo titular o su causante, relacionados parcial o totalmente con la invención de esta solicitud.
- ☐ De ser el caso, modificaciones efectuadas a la solicitud internacional.
- ☒ Otros: Reporte de búsqueda internacional, publicación y opinión escrita de la autoridad de búsqueda Internacional.

11

FIGURA CARACTERISTICA:



12

Solicito la concesión de la patente,

NOMBRE: ALICIA LLOREDA RICAURTE

FIRMA:

C.C. 39.690.713

T.P. 53.215

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800.176.089-2

- / -

RECIBO DE CAJA

Industria y Comercio
SUPERINTENDENCIA

No. 11 - 0052109

Bogotá D.C., Mayo 31 de 2011 - 06:51:19

RECIBIDO DE : LLOREDA & CIA. S.A.

NI 830.022.145

*** Soporte del Pago ***

TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	VR. PAGO
CONSIGNACION	BANCO DE BOGOTA	062754387	414999804	30/05/2011	24.532.000.00

*** Conceptos Pagados ***

CANT.	RENTISTICO	CONCEPTO	Vr. UNIDITARIO	Vr. CONCEPTO
1	50005-01-01 SOLICITUDES	1 TRAMITES DE SOL. DE PATENTE DE INVENCIÓN	571.000.00	571.000.00
				<u>\$571.000.00</u>

=====

SON: **QUINIENTOS SETENTA Y UN MIL PESOS MONEDA CORRIENTE***

Responsable: _____

Recibo de Caja Aplicado al Expediente No. _____

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 11-082169- -00000-0000

Fecha: 2011-06-30 16:57:06 Dep. 2020 DIR.NUEVASCR
 1 PATENTEIYII Eve: 378 FASENACIONALI
 PRESENTACION Folios: 49

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

Mayo 31 de 2011 - 06:51:30

 Industria y Comercio SUPERINTENDENCIA		SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DIVISIÓN DE NUEVAS CREACIONES EXTRACTO PARA PUBLICACIÓN SOLICITUD DE PATENTE DE INVENCION PCT	
(21) No. de solicitud:		(51) Int Cl: G06Q 20/00	
(22) Fecha de solicitud: 30-06-11		(71) Solicitante(s): MTN MOBILE MONEY SA (PTY) LTD	
(30) Prioridad	(31) No. Prioridad 2008/10835	(32) Fecha 23-12-08	(33) País ZA
		(72) Inventor(es): BRUYNSE, Dirk, Marinus y BEZUIDENHOUDT, Schalk, Johann.	
		(74) Apoderado: ALICIA LLOREDA RICAURTE	
(85) Fecha limite inicio fase nacional: 23-07-11		(87) Publicación internacional	
(86) Datos relativos a la presentación de la solicitud PCT		Fecha: 01-07-10	
Fecha de presentación de la solicitud: 18-12-09		No. publicación: WO 2010/073199 A1	
No. de solicitud: PCT/B2009/055838			
(54) Título: "MÉTODO Y SISTEMA PARA PROCESAR DE MANERA SEGURA UNA TRANSACCIÓN"			

Resumen - Reivindicación(es):

Sector: Sistemas o métodos de procesamiento de datos, especialmente adaptados para propósitos administrativos, comerciales, financieros, de gestión, de supervisión o de pronóstico, particularmente esquemas, arquitecturas o protocolos de pago.

Resumen.-

Un método para procesar de manera segura una transacción incluye almacenar una pluralidad de identificadores de instrumento de transacción financiera encriptados en una memoria en donde no hay clave de descifrado para estos almacenados en la memoria y además en donde los identificadores de instrumento de transacción financiera encriptadas están cada uno asociado con un dispositivo de comunicaciones móviles. Recibir en un servidor una solicitud para procesar una transacción, la solicitud incluyendo una identificación de un dispositivo de comunicación móviles. Retirar de la memoria el identificador de instrumento de transacción financiera encriptado asociado con el dispositivo de comunicaciones móviles identificado en la solicitud. Transmitir el identificador de instrumento de transacción financiera encriptado retirado al dispositivo de comunicaciones móviles. Recibir el dispositivo de comunicaciones móviles datos de transacción de dispositivo y usar los datos de transacción recibidos para efectuar una transacción financiera.



Industria y Comercio

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

DIVISIÓN DE NUEVAS CREACIONES

TARJETA ARCHIVO PROPIETARIOS

SUPERINTENDENCIA

PATENTE DE INVENCION ____ PCT X MODELO DE UTILIDAD ____ DISEÑO INDUSTRIAL ____

(21) No. de solicitud:

(22) Fecha de solicitud: 30-06-11

(51) Clasificación Internacional: G06Q 20/00

(71) Solicitante(s): **MTN MOBILE MONEY SA (PTY) LTD**

(72) Inventor(es): BRUYNSE, Dirk, Marinus y BEZUIDENHOUDT, Schalk, Johann.

(74) Apoderado: **ALICIA LLOREDA RICAURTE**

(30) Prioridad

(31)

No. Prioridad

(32)

Fecha

(33)

País

2008/10835

23-12-08

ZA

(85) Fecha límite inicio fase nacional: 23-07-11

(87) Publicación internacional

(86) Datos relativos a la presentación de la solicitud PCT

Fecha: **01-07-10**

Fecha de presentación de la solicitud: 18-12-09

No. publicación: **WO 2010/073199 A1**

No. de solicitud: **PCT/IB2009/055838**

(54) Título: **MÉTODO Y SISTEMA PARA PROCESAR DE MANERA SEGURA UNA TRANSACCIÓN.**



Industria y Comercio

SUPERINTENDENCIA

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

DIVISIÓN DE NUEVAS CREACIONES

TARJETA ARCHIVO TEMÁTICO

PATENTE DE INVENCION ____ PCT X MODELO DE UTILIDAD ____ DISEÑO INDUSTRIAL ____

(21) No. de solicitud: (22) Fecha de solicitud: 30-06-11

(51) Clasificación Internacional: G06Q 20/00

(71) Solicitante(s): MTN MOBILE MONEY SA (PTY) LTD

(72) Inventor(es): BRUYNSE, Dirk, Marinus y BEZUIDENHOUDT, Schalk, Johann.

(74) Apoderado: ALICIA LLOREDA RICAURTE

(30) Prioridad	(31) No. Prioridad	(32) Fecha	(33) País
	2008/10835	23-12-08	ZA

FIGURA CARACTERISTICA
6 x 6 cm

(85) Fecha limite inicio fase nacional: 23-07-11

(86) Datos relativos a la presentación de la solíc. PCT

Fecha de presentación de la solicitud: 18-12-09

No. de solicitud: PCT/IB2009/055838

(87) Publicación internacional:

Fecha: 01-07-10

No. Publicación : WO 2010/073199 A1

(54) Título: **MÉTODO Y SISTEMA PARA PROCESAR DE MANERA SEGURA UNA TRANSACCIÓN.**

(57) Resumen - Reivindicación(es):

Sector: Sistemas o métodos de procesamiento de datos, especialmente adaptados para propósitos administrativos, comerciales, financieros, de gestión, de supervisión o de pronóstico, particularmente esquemas, arquitecturas o protocolos de pago.

Resumen.-

Un método para procesar de manera segura una transacción incluye almacenar una pluralidad de identificadores de instrumento de transacción financiera encriptados en una memoria en donde no hay clave de descifrado para estos almacenados en la memoria y además en donde los identificadores de instrumento de transacción financiera encriptadas están cada uno asociado con un dispositivo de comunicaciones móviles. Recibir en un servidor una solicitud para procesar una transacción, la solicitud incluyendo una identificación de un dispositivo de comunicación móviles. Retirar de la memoria el identificador de instrumento de transacción financiera encriptado asociado con el dispositivo de comunicaciones móviles identificado en la solicitud. Transmitir el identificador de instrumento de transacción financiera encriptado retirado al dispositivo de comunicaciones móviles. Recibir el dispositivo de comunicaciones móviles datos de transacción de dispositivo y usar los datos de transacción recibidos para efectuar una transacción financiera.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference PA148406PCT	FOR FURTHER ACTION		sec Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/IB 09/55838	International filing date (day/month/year) 18 December 2009 (18.12.2009)	(Earliest) Priority Date (day/month/year) 23 December 2008 (23.12.2008)	
Applicant MTN MOBILE MONEY SA (PTY) LTD.			

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

a. With regard to the language, the international search was carried out on the basis of:

- ☒ the international application in the language in which it was filed.
☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b. ☐ This international search report has been established taking into account the rectification of an obvious mistake authorized by or notified to this Authority under Rule 91 (Rule 43.6b/s(a)).

c. ☐ With regard to any nucleotide and/or amino acid sequence disclosed in the international application, see Box No. I.

2. ☐ Certain claims were found unsearchable (see Box No. II).

3. ☐ Unity of invention is lacking (see Box No. III).

4. With regard to the title,

- ☒ the text is approved as submitted by the applicant.
☐ the text has been established by this Authority to read as follows:

5. With regard to the abstract,

- ☒ the text is approved as submitted by the applicant.
☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the drawings,

- a. the figure of the drawings to be published with the abstract is Figure No. 1
☒ as suggested by the applicant.
☐ as selected by this Authority, because the applicant failed to suggest a figure.
☐ as selected by this Authority, because this figure better characterizes the invention.
- b. ☐ none of the figures is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/IB 09/55838

A. CLASSIFICATION OF SUBJECT MATTER IPC(8) - G06Q 20/00 (2010.01) USPC - 705/64 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC(8): G06Q 20/00 (2010.01) USPC: 705/64 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched USPC: 705/78; 705/75 - search terms below. Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) WEST (PGPB, USPT, EPAB, JPAB) - finance, payment, purchase, transaction, transact, compensate, remunerate, fund, disbursement, deposit, remit, exchange, encrypt, security, protection, safeguarding, mobile, portable, removable, detachable, interchangeable, identifier, record, entry, candidate key, primary key, number, transaction key, server, decrypt		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008/0249948 A1 (KIM et al.) 09 October 2008 (09.10.2008) - abstract; para [0002]-[0003], [0006]-[0010], [0031], [0033], [0046]-[0047], [0049].	1-5, 9-13, 17-20
Y	US 2007/0198432 A1 (PITRODA et al.) 23 August 2007 (23.08.2007) - para [0180], [0356], [0369], [0392], [0405], [0412], [0511], [0681].	6-8, 14-16
Y	US 2007/0198432 A1 (PITRODA et al.) 23 August 2007 (23.08.2007) - para [0180], [0356], [0369], [0392], [0405], [0412], [0511], [0681].	6-8, 14-16
A	US 2008/0313061 A1 (LIMLENGCO) 18 December 2008 (18.12.2008).	1-20
A	US 2008/0301057 A1 (OREN) 04 December 2008 (04.12.2008).	1-20
A	US 2008/0177668 A1 (DELEAN) 24 July 2008 (24.07.2008).	1-20
A	US 2008/0091616 A1 (HELWIN et al.) 17 April 2008 (17.04.2008).	1-20
A	US 6,766,161 B2 (GEISELMAN et al.) 20 July 2004 (20.07.2004).	1-20
☐ Further documents are listed in the continuation of Box C. ☐		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 21 April 2010 (21.04.2010).		Date of mailing of the international search report 14 MAY 2010
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201		Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

- (51) International Patent Classification:
G06Q 20/00 (2006.01)
- (21) International Application Number:
PCT/IB2009/055838
- (22) International Filing Date:
18 December 2009 (18.12.2009)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
2008/10835 23 December 2008 (23.12.2008) ZA
- (71) Applicant (for all designated States except US): MTN
MOBILE MONEY SA (PTY) LTD [ZA/ZA]; 216 14th
Avenue, 2022 Fairlands (ZA).
- (72) Inventors; and
(75) Inventors/Applicants (for US only): BRUYNSE, Dirk,
Marinus [ZA/ZA]; 43 Dianne Road, Olivedale, 2158 Jo-
hannesburg (ZA). BEZUIDENHOUDT, Schalk, Johann
[ZA/ZA]; 5 Cliffside Crescent, 2115 Northcliff (ZA).
- (74) Agents: SPOOR & FISHER et al.; P O Box 454, 0001
Pretoria (ZA).
- (81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP,
KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD,
ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,
NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD,
SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT,
TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,
ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ,
TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
ML, MR, NE, SN, TD, TG).

Published:

- with international search report (Art. 21(3))
- before the expiration of the time limit for amending the
claims and to be republished in the event of receipt of
amendments (Rule 48.2(h))

(54) Title: METHOD OF AND SYSTEM FOR SECURELY PROCESSING A TRANSACTION

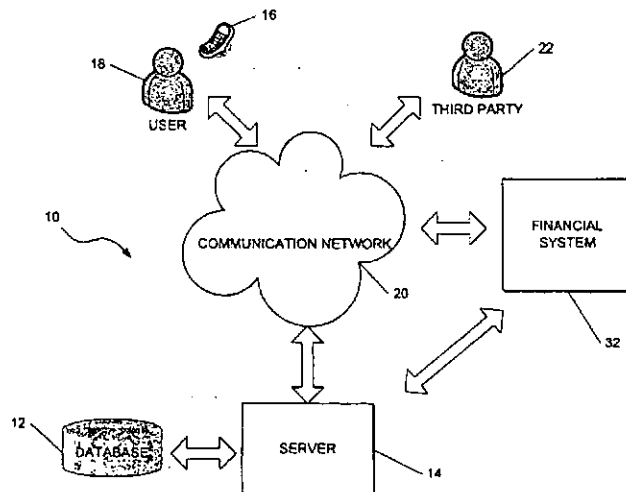


FIGURE 1

(57) Abstract: A method of securely processing a transaction includes storing a plurality of encrypted financial transaction instrument identifiers in a memory wherein there is no decryption key for these stored in the memory and further wherein the encrypted financial transaction instrument identifiers are each associated with a mobile communications device. Receiving at a server a request to process a transaction, the request including an identification of a mobile communications device. Retrieving from the memory the encrypted financial transaction instrument identifier associated with the mobile communications device identified in the request. Transmitting the retrieved encrypted financial transaction instrument identifier to the mobile communications device. Receiving from the mobile communications device transaction data and using the received transaction data to effect a financial transaction.

From the
INTERNATIONAL SEARCHING AUTHORITY

To: SPOOR & FISHER
PO BOX 454
0001 PRETORIA
SOUTH AFRICA

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing
(day/month/year)

14 MAY 2010

Applicant's or agent's file reference
PA148406PCT

FOR FURTHER ACTION

See paragraph 2 below

International application No.

PCT/IB 09/55838

International filing date (day/month/year)

18 December 2009 (18.12.2009)

Priority date (day/month/year)

23 December 2008 (23.12.2008)

International Patent Classification (IPC) or both national classification and IPC

IPC(8) - G06Q 20/00 (2010.01)

USPC - 705/64

Applicant **MTN MOBILE MONEY SA (PTY) LTD.**

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450
Facsimile No. 571-273-3201

Date of completion of this opinion

21 April 2010 (21.04.2010).

Authorized officer:

Lee W. Young

PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

PCT/IB2009/055838 14.05.2010

International application No.
PCT/IB 09/55838

Box No. I Basis of this opinion

1. With regard to the language, this opinion has been established on the basis of:
 - ☒ the international application in the language in which it was filed.
 - ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).
2. ☐ This opinion has been established taking into account the rectification of an obvious mistake authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))
3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:
 - a. (means)
 - ☐ on paper
 - ☐ in electronic form
 - b. (time)
 - ☐ in the international application as filed
 - ☐ together with the international application in electronic form
 - ☐ subsequently to this Authority for the purposes of search
4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5. Additional comments:

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/IB 09/55838

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**1. Statement**

Novelty (N)	Claims	6-8, 14-16	YES
	Claims	1-5, 9-13, 17-20	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-20	NO
Industrial applicability (IA)	Claims	1-20	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-5, 9-13, and 17-20 lack novelty under PCT Article 33(2) as being anticipated by US 2008/0249948 A1 to KIM et al. (hereinafter 'Kim').

As per claim 1, Kim discloses:

a method of securely processing a transaction, the method including:
storing a plurality of encrypted financial transaction instrument identifiers in a memory (para [0007], [0009]-[0010])
wherein there is no decryption key for these stored in the memory (para [0006], [0009]-[0010]) and
further wherein the encrypted financial transaction instrument identifiers are each associated with a mobile communications device (para [0006], [0009]-[0010]);
receiving at a server a request to process a transaction (para [0010]),
the request including an identification of a mobile communications device (para [0009]-[0010]);
retrieving from the memory the encrypted financial transaction instrument identifier associated with the mobile communications device identified in the request (para [0009]-[0010]);
transmitting the retrieved encrypted financial transaction instrument identifier to the mobile communications device (para [0010]);
receiving from the mobile communications device transaction data and using the received transaction data to effect a financial transaction (para [0007]-[0010]).

As per claim 9, Kim discloses:

a system for processing a transaction, the system including:
a memory storing a plurality of encrypted financial transaction instrument identifiers (para [0007], [0009]-[0010])
wherein there is no decryption key for these stored in the memory (para [0006], [0009]-[0010]) and
further wherein the encrypted financial transaction instrument identifiers are each associated with a mobile communications device (para [0006], [0009]-[0010]);
a communications module to receive a request to process a transaction (para [0010]),
the request including an identification of a mobile communications device (para [0009]-[0010]);
a retrieving module to retrieve from the memory the encrypted financial transaction instrument identifier associated with the mobile communications device identified in the request (para [0009]-[0010]) and to pass this to the communications module for transmitting to the mobile communications device (para [0010]); and
a data formatting module in communication with the communications module to receive from the mobile communications device transaction data and to use the received transaction data to effect a financial transaction (para [0007]-[0010]).

As per claim 17, Kim discloses:

a method of securely processing a transaction, the method including:
storing on a mobile communications device a key to decrypt an encrypted financial transaction instrument identifier (para [0006]-[0007], [0009]-[0010]);
receiving at the mobile communications device an encrypted financial transaction instrument identifier (para [0009]-[0010]);
decrypting the encrypted financial transaction instrument identifier (para [0010]);
displaying to a user of the mobile communications device the financial transaction instrument identifier together with information relating to a financial transaction (para [0007]-[0010], [0031], [0033], [0049]);
prompting the user to enter an authentication PIN (abstract - customer's identification number; para [0003] - card identification number; para [0006], [0009]-[0010] - telephone number; [0046]-[0047]);
encrypting the authentication PIN and transmitting this over a communications network to a server thereby to instruct the server to process the financial transaction identified to the user (para [0007]-[0010]).

-- supplemental page --

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

PCT/IB2009/055838 14.05.2010

International application no.

PCT/IB 09/55838

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:
Box V

As per claims 2 and 10, Kim further discloses that:
the transaction data received from the mobile communications device includes a decryption key to decrypt a stored encrypted financial transaction instrument identifier associated with the mobile communications device (para [0006]-[0007], [0009]-[0010]).

As per claims 3 and 11, Kim further discloses that:
the transaction data received from the mobile communications device includes a financial transaction instrument identifier to be used to effect the financial transaction (para [0003], [0007]-[0010], [0031], [0046]-[0047]).

As per claims 4 and 12, Kim further discloses:
the receiving of a PIN from the mobile communications device to authorize a financial transaction (abstract - customer's identification number; para [0003] - card identification number; para [0006], [0009]-[0010] - telephone number; [0046]-[0047]).

As per claims 5 and 13, Kim further discloses that:
the PIN is received via a different communication channel to the transaction data received from the mobile communications device (para [0003], [0006], [0009]-[0010], [0046]-[0047]).

As per claim 18, Kim further discloses that:
the key to decrypt the encrypted financial transaction instrument identifier is the same key that is stored in a memory on the mobile communications device and used by the mobile communications device to authenticate communications over a mobile communications network (abstract, para [0002], [0009]-[0010] -- symmetric key algorithm).

As per claim 19, Kim further discloses that:
the financial transaction instrument identifier and authentication PIN are transmitted over different communications networks to the server (para [0003], [0006], [0009]-[0010], [0046]-[0047]).

As per claim 20, Kim discloses:
a mobile communications device including:
a memory having stored on a mobile communications device a key to decrypt an encrypted financial transaction instrument identifier (para [0006]-[0007], [0009]-[0010]);
a receiving module to receive at the mobile communications device an encrypted financial transaction instrument identifier (para [0009]-[0010]);
a decrypting module to decrypt the encrypted financial transaction instrument identifier (para [0010]);
a display to display to a user of the mobile communications device the financial transaction instrument identifier together with information relating to a financial transaction (para [0007]-[0010], [0031], [0033], [0049]);
a data input module to receive from the user an authentication PIN (abstract - customer's identification number; para [0003] - card identification number; para [0006], [0009]-[0010] - telephone number; [0046]-[0047]); and
an encryption module to transmit the PIN over a communications network to a server thereby to instruct the server to process the financial transaction identified to the user (para [0007]-[0010]).

Claims 6-8 and 14-16 lack an inventive step under PCT Article 33(3) as being obvious over Kim in view of US 2007/0198432 A1 to PITRODA et al. (hereinafter 'Pitroda').

As per claims 6 and 14, Kim discloses the features of claims 1 and 10 as discussed above. Kim does not disclose that the transaction data received from the mobile communications device includes one or more of: third party identification data that identifies a third party to whom an amount is to be paid; and the amount to be paid to the third party. However, Pitroda discloses that the transaction data received from the mobile communications device includes one or more of:
third party identification data that identifies a third party to whom an amount is to be paid; and
the amount to be paid to the third party (para [0180], [0392], [0681]). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to add the feature of Pitroda to Kim in order to associate an enterprise portal with securely transmitting third-party quotes and bids (para [0180]).

As per claims 7 and 15, Kim discloses the features of claims 1 and 10 as discussed above. Kim does not disclose that the method further comprises using the received transaction data from the mobile communications device to create a transaction data packet to be transmitted to a financial system that uses the transaction data packet to effect the financial transaction. However, Pitroda discloses that the method further comprises using the received transaction data from the mobile communications device to create a transaction data packet to be transmitted to a financial system that uses the transaction data packet to effect the financial transaction (para [0356], [0369], [0405], [0412], [0511]). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to add the feature of Pitroda to Kim in order to provide any needed degree of connectivity between incompatible physical, programming, protocol-based or other interfaces to a service facility (para [0356], [0369]).

As per claims 8 and 16, Pitroda further discloses that:
the transaction data packet is structured in the same format as a card present data packet so that the financial system can treat the financial transaction as a card present transaction (para [0356], [0369], [0405], [0412], [0511]).

Claims 1-20 have industrial applicability as defined by PCT Article 33(4), because the subject matter can be made or used in industry.

MÉTODO Y SISTEMA PARA PROCESAR DE MANERA SEGURA UNA TRANSACCIÓN

RESUMEN-OBJETO Y FINALIDAD DE LA INVENCION

Un método para procesar de manera segura una transacción incluye

5 almacenar una pluralidad de identificadores de instrumento de transacción financiera encriptados en una memoria en donde no hay clave de descifrado para estos almacenados en la memoria y además en donde los identificadores de instrumento de transacción financiera encriptados están cada uno asociado con un dispositivo de comunicaciones móviles. Recibir en un servidor una solicitud para

10 procesar una transacción, la solicitud incluyendo una identificación de un dispositivo de comunicaciones móviles. Retirar de la memoria el identificador de instrumento de transacción financiera encriptado asociado con el dispositivo de comunicaciones móviles identificado en la solicitud. Transmitir el identificador de instrumento de transacción financiera encriptado retirado al dispositivo de

15 comunicaciones móviles. Recibir del dispositivo de comunicaciones móviles datos de transacción de dispositivo y usar los datos de transacción recibidos para efectuar una transacción financiera.

SECTOR: Sistemas o métodos de procesamiento de datos, especialmente

20 adaptados para propósitos administrativos comerciales, financieros, de gestión, de supervisión o de pronóstico, particularmente esquemas, arquitecturas o protocolos de pago.

MÉTODO Y SISTEMA PARA PROCESAR DE MANERA SEGURA UNA TRANSACCIÓN

ANTECEDENTES DE LA INVENCION

Esta invención se relaciona con un método para y sistema para
5 procesar de manera segura una transacción, usando particularmente un
dispositivo de comunicaciones móvil.

Se conoce un número de métodos para procesar transacciones
usando dispositivo de comunicaciones móvil. Sin embargo, ninguno de estos
ofrece una solución segura que sea fácil de usar y efectiva.

10 Un objeto de la invención es proporcionar un método y sistema
mejorados para procesar de manera segura una transacción.

COMPENDIO DE LA INVENCION

De conformidad con un primer aspecto de la invención, existe un
método para procesar de manera segura una transacción del método incluyendo:

15 almacenar una pluralidad de identificadores de instrumento de
transacción financiera encriptados en una memoria en donde no hay clave de
descripción para estos almacenados en la memoria y además en donde los
identificadores de instrumento de transacción financiera encriptados están cada
uno asociado con un dispositivo de comunicaciones móvil;

recibir en un servidor una solicitud para procesar una transacción, la solicitud incluyendo una identificación de un dispositivo de comunicaciones móvil;

retirar de la memoria el identificador de instrumento de transacción financiera encriptado asociado con el dispositivo de comunicaciones móvil
5 identificado en la solicitud; transmitir el identificador de instrumento de transacción financiera encriptado retirado al dispositivo de comunicaciones móvil; recibir del dispositivo de comunicaciones móvil dato de transacción y usar el dato de transacción recibido para efectuar una transacción financiera.

El dato de transacción recibido del dispositivo de comunicaciones
10 móvil puede incluir una clave de descripción para descifrar un identificador de instrumento de transacción financiera encriptado almacenado asociado con el dispositivo de comunicaciones móvil.

Alternativamente o en adición, el dato de transacción recibido del dispositivo de comunicaciones móvil incluye un identificador de instrumento de
15 transacción financiera para usarse para efectuar la transacción financiera.

De preferencia el método incluye recibir un PIN para el dispositivo de comunicaciones móvil para autorizar una transacción financiera.

El dato de transacción recibido del dispositivo de comunicaciones móvil puede incluir uno o más de:

20 identificación de tercera parte que idéntica a una tercera pagar a quien se va a pagar una cantidad; y la cantidad a pagar a la tercera parte.

El método puede comprender además usar el dato de transacción recibido del dispositivo de comunicaciones móvil para crear un paquete de datos de transacción que se va a transmitir a un sistema financiero que usa el paquete de datos de transacción para efectuar la transacción financiera.

5 En un ejemplo, el paquete de datos de transacción está estructurado en el mismo formato que un paquete de datos presente de tarjeta de modo que el sistema financiero pueda tratar la transacción financiera como una transacción de presentación de tarjeta.

De conformidad con un segundo aspecto de la invención hay un
10 sistema para procesar de manera segura una transacción, el sistema incluyendo:

una memoria que almacena una pluralidad de identificadores de
instrumento de transacción financiera encriptados en donde no hay clave de
descripción para estos almacenados en la memoria y además en donde los
identificadores de instrumento de transacción financiera encriptados están cada
15 uno asociados con un dispositivo de comunicaciones móvil;

un módulo de comunicaciones para recibir una solicitud para procesar una
transacción, la solicitud incluyendo una identificación de un dispositivo de
comunicaciones móvil;

un módulo de retiro para retirar de la memoria el identificador de
20 instrumento de transacción financiera encriptado asociado con el dispositivo de

comunicaciones móvil en la solicitud y para pasar este al módulo de comunicaciones para transmitir al dispositivo de comunicaciones móvil, y

un módulo de formato de datos en comunicación con el módulo de comunicaciones para recibir del dispositivo de comunicaciones móvil datos de transacción y usar el dato de transacción recibido para efectuar una transacción financiera.

El módulo de comunicaciones puede recibir además datos de transacción del dispositivo de comunicaciones móvil, cuyo dato de transacción incluye una clave de descripción para descifrar un identificador de instrumento de transacción financiera encriptado almacenado, asociado con el dispositivo de comunicaciones móvil.

Alternativamente o en adición, el módulo de comunicaciones recibe además dato de transacción del dispositivo de comunicaciones móvil, cuyo dato de transacción incluye un identificador de instrumento de transacción financiera que se va a usar para efectuar la transacción financiera.

De preferencia, el módulo de comunicaciones recibe además un PIN del dispositivo de comunicaciones móvil para autorizar una transacción financiera.

El módulo de comunicaciones puede recibir el PIN a través de un canal de comunicación diferente al dato de transacción recibido del dispositivo de comunicaciones móvil.

En un ejemplo, el dato de transacción recibido del dispositivo de comunicaciones móvil incluye uno o más de:

dato de identificación de tercera parte que identifica una tercera parte a quien se va a pagar una cantidad; y la cantidad a pagar a la tercera parte.

5 El módulo de formatear dato puede usar además el dato de transacción recibido del dispositivo de comunicaciones móvil para crear un paquete de dato de transacción que se va a transmitir a un sistema financiera que usa el paquete de datos de transacción para efectuar la transacción financiera.

De preferencia, el módulo de formatear dato estructura el paquete de
10 dato de transacción en el mismo formato que un paquete de dato de presentación de tarjeta de modo que el sistema financiero puede tratar la transacción financiera como una tracción de presentación de tarjeta.

De conformidad con un tercer aspecto de la invención, hay un método para procesar de manera segura una transacción, el método incluyendo:

15 almacenar en un dispositivo de comunicaciones móvil una clave para descifrar un identificador de instrumento de transacción financiera encriptado; recibir en el dispositivo de comunicaciones móvil un identificador de instrumento de transacción financiera encriptado; descifrar el identificador de instrumento de transacción financiera encriptado, presentar a un
20 usuario del dispositivo de comunicaciones móvil el identificador de instrumento de transacción financiera junto con información relacionada con una transacción

financiera; avisar al usuario que de e3ntrada a un PIN de autenticación; encriptar el PIN de autenticación y transmitir este a través de una red de comunicaciones a un servidor para de esta manera instruir al servidor que procese la transacción financiera identificada al usuario.

5 La clave para descifrar el identificador de instrumento de transacción financiera encriptado puede ser la misma clave que está almacenada en una memoria en el dispositivo de comunicaciones móvil y usada por el dispositivo de comunicaciones móvil para autenticar comunicaciones a través de una red de comunicaciones móvil.

10 Además, el identificador de instrumento de transacción financiera y PIN de autenticación se pueden transmitir a través de diferentes redes de comunicaciones al servidor.

De conformidad con un segundo aspecto de la invención hay un sistema para procesar de manera segura una transacción, el sistema incluyendo:

15 una memoria que tiene almacenado en un dispositivo de comunicaciones móvil una clave para descifrar un identificador de instrumento de transacción financiero encriptado;

un módulo receptor para recibir en el dispositivo de comunicaciones móvil un identificador de instrumento de transacción financiera encriptado;

20 un módulo de descifrado para descifrar el identificador de instrumento de transacción financiera encriptado;

una presentación para presentar a un usuario del dispositivo de comunicaciones móvil el identificador de instrumento de transacción financiera junto con información relacionada con una transacción financiera;

un módulo de entrada de dato para recibir el usuario un PIN de
5 autenticación; y

un módulo de encriptación para transmitir el PIN a través de una red de comunicaciones a un servidor para de esta manera instruir al servidor de procesar la transacción financiera identificada al usuario.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

10 La Figura 1 muestra un diagrama esquemático de un sistema de conformidad con una modalidad de ejemplo;

La Figura 2 muestra un diagrama de bloque del servidor de la Figura 1 con mayor detalle;

La Figura 3 muestra un diagrama de flujo de un método de
15 conformidad con una modalidad de ejemplo;

La Figura 4 muestra un diagrama de flujo de un método de ejemplo de uso para la presente invención; y

La Figura 5 muestra un diagrama de bloque de un dispositivo de comunicaciones móvil de ejemplo.

DESCRIPCIÓN DE MODALIDADES PREFERIDAS

En la siguiente descripción, para propósitos de explicación, numerosos detalles específicos se exponen a fin de proporcionar un entendimiento completo de una modalidad de la presente exposición. Será evidente, sin embargo, a uno experto en el ramo que la presente exposición se puede practicar sin estos detalles específicos.

Haciendo referencia a las Figuras que se acompañan en donde un sistema y método de conformidad con la invención se describen, el sistema 10 incluye una memoria 12 en la que está almacenada una pluralidad de identificadores de instrumento de transacción financiera encriptados.

Lo que es importante y lo que se explicar con mayor detalle más adelante es que no hay clave de descifrado para estos identificadores de instrumento de transacción financiera encriptados almacenados en la memoria 12 o en el servidor 14 asociado.

Esto significa que ni la memoria 12 ni el servidor 143 asociado es capaz de descifrar estos para extraer identificadores de instrumento de transacción financiera almacenados en los mismos.

Además, cada identificador de instrumento de transacción financiera encriptado está asociado de manera única con un dispositivo 16 de comunicaciones móvil de un usuario 18.

Para conveniencia, solamente un solo dispositivo 16 de comunicaciones móvil y usuario 18 se ilustran en la Figura 1, sin embargo en la práctica, habrá una pluralidad de dispositivos 16 de comunicaciones móvil cada uno asociado de manera única con una pluralidad de usuarios 18.

5 Uno de los objetivos de la presente invención es permitir al usuario 18 utilizar el dispositivo 16 de comunicaciones móvil para una transacción financiera de una manera segura. En la metodología abajo descrita, la transacción financiera se ilustrará como un pago por artículos o servicios, pero se apreciará que esto es para propósitos de ejemplo solamente y que otros tipos de
10 transacciones financieras podrían implementarse igualmente usando el sistema y metodología descritos en la presente.

Además, el instrumento de transacción financiera podría ser una tarjeta de crédito o débito, por ejemplo.

A fin de obtener los identificadores de instrumento de transacción
15 financiera y asociarlos con dispositivos de comunicaciones móviles, el usuario 18 será requerido para registrarse a fin de usar el sistema.

Antes de registrarse, el usuario debe tener un identificador de instrumento de transacción financiera válido tal como una tarjeta de débito o crédito asociada con una cuenta de tarjeta de débito o crédito, por ejemplo. Aún
20 cuando el uso de una sola tarjeta de débito o crédito por usuario se describirá

ahora, el sistema también es capaz de acomodar una pluralidad de tarjetas por usuario.

El usuario, luego tiene acceso al servidor 14 a

través de un canal de comunicación para conducir el proceso de registro.

5 El servidor 14 ilustrado con mayor detalle en el diagrama de bloque de la Figura 2 incluye un módulo 24 de comunicaciones para propósitos de esta y otras comunicaciones que el servidor lleva a cabo como se describirá abajo con mayor detalle.

El canal de comunicación usado para el proceso de comunicación
10 podría ser el mismo canal 20 de comunicación usado para procesar transacciones o podría ser otro canal de comunicaciones.

En la modalidad ilustrada, el canal 20 de comunicación incluye una red de comunicaciones móviles.

Cuando el usuario utiliza su dispositivo 16 de comunicaciones móvil y
15 el canal 20 de comunicaciones, un número de protocolos están disponibles incluyendo marcar hacia un servidor en respuesta de voz interactiva (IVR), acoplarse en un proceso de Dato de Servicio Suplementario No Estructurado (USSD), usando un protocolo de Aplicación Inalámbrica (WAP) o de Puerta de Internet Inalámbrica (WIG) para tener acceso al servidor 14, para mencionar
20 solamente unos pocos ejemplos.

Evidentemente, el usuario podría usar una red de comunicaciones diferente y protocolo para completar el proceso de registro arriba mencionado.

En cualquier caso, el servidor 14 u otro servidor asociado con el
5 servidor 14 incluirá hardware y software para permitir al usuario tener acceso al servidor y completar el proceso de registro.

Para propósitos de ilustración, el proceso de registro se describirá como se implementa por el servidor 14.

El servidor 14 recibe la solicitud de registro y detecta la identidad del
10 dispositivo de comunicaciones móviles tal como el Número de Directorio de Suscriptor Internacional de Estación Móvil (MSISDN) del dispositivo, por ejemplo.

Cuando el usuario no está usando el dispositivo de comunicaciones móvil para registro, serán avisados de dar entrada a la identidad del dispositivo 16 de comunicaciones móviles.

15 El servidor 14 valida que la identidad del dispositivo de comunicaciones móviles es válido comprobando la identidad con la red 20 de comunicaciones móviles.

El usuario 18 es ahora avisado de dar entrada a detalles de identificación personal tales como su número de identidad.

Además, el usuario es avisado de dar entrada a detalles de instrumento de transacción financiera. En la modalidad ilustrada de una tarjeta de crédito o una tarjeta de débito, el usuario da entrada a uno o más del tipo de tarjeta, el número de tarjeta, la fecha de expiración de la tarjeta, y una cuenta asociada con la tarjeta.

5 Cuando se obtiene un número de cuenta del usuario, la cuenta también puede ser comprobada para un balance positivo de fondos disponibles por el servidor 14.

Una vez que la información es recibida en el servidor 14, la información se transmite de manera segura nuevamente al usuario para
10 confirmación en su dispositivo 16 de comunicaciones móviles a través de la red 20 de comunicaciones.

El usuario confirma que la información es correcta y luego es avisado adicionalmente de su dispositivo 16 de comunicaciones móviles que entre a uno de un número de PIN asociado con la tarjeta y un valor de cheque presentado en
15 la tarjeta conocido como el valor CV2, CVV o CVC.

Toda la información de instrumento de transacción financiera arriba descrita luego se encripta por el dispositivo 16 de comunicaciones móviles, se transmite a través de la red 20 de comunicaciones al servidor 14 y se almacena en la memoria 12 asociada con la información personal y dispositivo 16 de
20 comunicaciones móviles.

Como se describe arriba, la clave de descifrado no está almacenado en la memoria 12 ni en ninguna otra memoria asociada con el servidor 14. Más bien, la clave de descifrado está almacenada solamente en una memoria del dispositivo 16 de comunicaciones móviles con el que está asociado el instrumento de transacción financiera. Típicamente, la memoria está colocada en el SIM del dispositivo 16 de comunicaciones móviles.

En una modalidad de ejemplo esta clave de descifrado es la misma que las claves que están cargadas a la tarjeta SIM en el punto de fabricación en un ambiente seguro para permitir que la tarjeta SIM se comuniquen de manera segura a través de la red de comunicaciones. La función primaria de las claves es prevenir el uso ilegal de la infraestructura de red móvil y la presente invención se respalda en estas claves. Se apreciará que las claves cargadas después del proceso de fabricación pueden ser más fácilmente comprometidas.

De esta manera una estructura o bloque de dato seguro se crea que es accesible de manera única por el SIM del dispositivo 16 de comunicaciones móviles, pero no está almacenado en el dispositivo 16 de comunicaciones móviles. Este bloque de dato seguro que contiene el identificador de instrumento de transacción financiera encriptado se almacena en el servidor 14 que no es capaz de tener acceso al bloque así como no tiene acceso a la clave de descifrado.

Una vez que el usuario se registra son capaces de conducir transacciones financieras usando un dispositivo 16 de comunicaciones móvil como el mecanismo para conducir la transacción.

En el ejemplo abajo, la transacción financiera se describirá como la compra de un producto o servicio en donde el dispositivo 16 de comunicaciones móvil se usa luego para pagar por el producto o servicio. Sin embargo, se apreciará que la transacción financiera podría ser cualquier otra clase de transacción financiera y no está limitada a una transacción de pago.

Para propósitos de ilustración, el pago se hace a una tercera parte 22 que tiene una cuenta de una clase u otra con una institución financiera. La tercera parte 22 puede o no estar conectada en la red 20 de comunicaciones.

En cualquier caso, el usuario inicia la transacción financiera enviando un mensaje de solicitud de transacción al servidor 14. El mensaje puede ser enviado usando el dispositivo 16 de comunicaciones móviles y la red 20 de comunicaciones o el mensaje se podría enviar al servidor usando otro canal de comunicaciones. Una modalidad de este inicio se muestra en la primera parte del proceso en la Figura 4.

Si otro canal de comunicaciones se usa, la identificación del dispositivo 16 de comunicaciones móvil necesitará ser enviada a través con la solicitud. Si el mensaje se envía del dispositivo 16 de comunicaciones móviles la identidad del dispositivo 16 de comunicaciones móviles será típicamente capaz de ser extraída del mensaje. Esto se hace normalmente detectando el Número de Directorio de suscriptor Internacional de Estación Móvil (MSISDN) del dispositivo, por ejemplo.

En cualquier caso, la solicitud es recibida en el servidor 14. Esta solicitud actúa como el percutor para ajustar el proceso de transacción financiera.

En respuesta a un percutor, un módulo 26 de retiro del servidor 14 retira de la memoria 12 el identificador de instrumento de transacción financiera encriptado asociado con el dispositivo 16 de comunicaciones móvil desde el que
5 se recibió la solicitud o identificado en la solicitud recibida. Usando el módulo 24 de comunicación, el

Identificador de instrumento de transacción financiera encriptado retirado se transmite al dispositivo 16 de comunicaciones móvil identificado a través de la red
10 20 de comunicaciones.

Como se describe arriba, el dispositivo 16 de comunicaciones móvil tiene almacenada en el mismo la clave para descifrar al identificador de instrumento de transacción financiera encriptado recibido del servidor 14.

En una modalidad de ejemplo, cuando menos algo de la información
15 de instrumento de transacción financiera se muestra al usuario en el dispositivo 16 de comunicaciones móvil para que el usuario confirme que se va a usar el instrumento de transacción financiera correcto.

Esto se muestra típicamente al usuario junto con alguna información perteneciente a la transacción financiera particular de modo que el usuario pueda
20 confirmar adicionalmente que este instrumento de transacción financiera se debe usar para esta transacción financiera.

Luego se pide al usuario que de entrada a su PIN para autenticar la transacción, cuyo PIN es transmitido nuevamente al servidor 14 como se describirá abajo con mayor detalle.

E. PIN y otros elementos necesarios para efectuar

- 5 la transacción luego se ponen en cifra de una manera que solamente el servidor 14 puede tener acceso y luego enviar a través de la red 20 de comunicación al servidor 14.

Parte de la información obtenida del identificador de instrumento de transacción financiera descifrado se combina en el dispositivo 16 de
 10 comunicaciones móvil con la otra información de transacción que incluye uno o más de datos de identificación de la tercera parte que4 identifica una tercera parte a quien una cantidad se va a pagar y la cantidad a pagar a la tercera parte.

Alternativamente, la otra información incluyendo detalles de la tercera parte y cantidad que se va a pagar se puede transmitir al servidor 14
 15 separadamente aún cuando esto restaría el nivel de seguridad a la transacción ya que separar la información del momento de autenticación permite espalme de transacción y de esta manera manipulación de transacción.

El dispositivo 16 de comunicaciones móvil de esta manera construye un paquete de datos de transacción encriptado y envía este al servidor 14.

El paquete de datos de transacción encriptado no es una transacción financiera completa sino que solamente incluye componentes de la misma y así el servidor 14 construye adicionalmente la transacción y la envía a través al banco para autenticación. Un ejemplo de lo que el paquete de datos puede incluir es

5 como sigue:

Primer Juego de Datos

Remitentes de MSISDN

Recipiente de MSIADN (identidad del recipiente en este ejemplo)

Cantidad de Transacción

10 Claves MSISDN

Segundo Juego de Datos

Remitentes de MSISDN

Claves de MSISDN

PIN

15 CVV

En la modalidad de ejemplo, el dato transmitido nuevamente del dispositivo móvil está en el paquete de datos encriptados se envía al servidor 14 a través de un canal de comunicación mientras que el usuario dio entrada al PIN se

envía al servidor 14 a través de otro canal de comunicaciones que es por lo que el ejemplo anterior tiene dos juegos de datos.

Se apreciará que esto añade seguridad a la transacción ya que el paquete de dato encriptado no se puede usar sin el PIN y el PIN es inútil con el
5 paquete de dato encriptado.

Los dos canales diferentes ambos podrían ser canales seguros o uno o más de los canales podría ser un canal inseguro.

En la modalidad ilustrada, el paquete de dato encriptado se envió a través de un canal USSD que es un ejemplo de un canal relativamente inseguro,
10 mientras que el PIN se envió a través de un canal WIG que es un canal relativamente seguro.

Esto es debido a que el canal WIG usa claves incrustadas en la memoria del dispositivo de comunicaciones como se describe arriba para autenticar la comunicación. Otro ejemplo de un canal seguro es SAD que también
15 usa claves de autenticación.

De esta manera, en una modalidad de ejemplo, el PIN de autenticación se transmite desde el dispositivo 16 de comunicaciones móvil a través de un canal seguro en una manera que cada transmisión es única y el servidor 14 mientras que valida el PIN también asegura la calidad única de
20 transmisión para asegurar que el bloque de transacción completo y o el PIN no se

pueda someter nuevamente. Esto se hace para detener ataques de reproducción y nuevo uso de

PINs.

Una vez que el servidor 14 recibe el bloque de PIN de autenticación
5 del dispositivo 16 de comunicaciones móvil, comprueba que el bloque de PIN sea correcto usando el módulo 28 de comprobación de PIN. Este bloque de PIN también será enviado posteriormente a la institución financiera para comprobación adicional.

Si el PIN es correcto, el servidor 14 entonces descifra el paquete de
10 datos de transacción asegurado recibido.

El servidor 14 usa la identidad del dispositivo de comunicaciones móvil para tener acceso a los detalles de identificador de instrumento de transacción financiera completos que todavía están encriptados y no son accesibles al servidor 14 sin el bloque de datos de transacción asegurado recibido
15 del dispositivo de comunicación móvil.

El bloque de datos del dispositivo móvil permite que el servidor extraiga los detalles de identificadores de instrumento de transacción financiera encriptado para nueva formación de paquete.

En una modalidad de ejemplo, las claves recibidas del dispositivo de
20 comunicaciones móvil permiten que el servidor descifre los detalles de identificadores de instrumento de transacción financiera almacenados asociados

con el MSISDN y cree una transacción financiera para transmisión posterior al banco.

En una modalidad alternativa, el identificador de instrumento de transacción financiera se transmite nuevamente al servidor mediante el dispositivo de comunicaciones móvil para uso por el servidor.

El servidor 14 de esta manera usa el dato recibido, junto con el identificador de instrumento de transacción financiera para crear un paquete de datos que se va a transmitir a un sistema 32 financiero que usa el paquete de datos para efectuar la transacción financiera.

En un ejemplo, el dato recibido del dispositivo 16 de comunicaciones móvil se recibe en el formato correcto para enviarse al sistema 32 financiero.

En otra modalidad de ejemplo, el dato recibido del dispositivo 16 de comunicaciones móvil no se recibe en el formato correcto para ser enviado al sistema financiero y se formatea nuevamente mediante un módulo 30 de formateo de datos antes de ser enviado al sistema 32 financiero.

En cualquier caso, el paquete de datos está estructurado en el mismo formato que un paquete de datos de presentación de tarjeta de manera que el sistema financiero puede tratar la transacción financiera como una transacción de presentación de tarjeta.

Se debe apreciar que "módulo" en el contexto de la especificación incluye una porción identificable de código, instrucciones computacionales o

ejecutables, datos, u objeto computacional para lograr una función particular, operación, procesamiento o procedimiento. Un módulo no necesita ser implementado en software solo, sino que un módulo se puede implementar en software y/o9 firmware y/o hardware.

5 En un ejemplo ilustrado en la Figura 4, el método y sistema se usan para comprar tiempo aire mediante lo cual una solicitud de compra de tiempo aire se ensambla por el usuario típicamente usando su dispositivo 16 de comunicaciones móviles y se transmite al servidor 143 o un servidor asociado – la primera porción de la Figura 4.

10 La solicitud es validada y el usuario luego es avisado de dar entrada al número de dispositivo de comunicaciones móviles del recipiente. Se apreciará que el usuario podría dar entrada aquí a su propio número y comprar tiempo aire para si mismos.

 El número recibido al que el usuario ha dado entrada se comprueba
15 para ver si existe.

 El dato de transacción completo y el identificador de instrumento de transacción financiera encriptado luego se envían del servidor 14 a través de la red 20 de comunicación al dispositivo 16 de comunicaciones móviles identificado en donde el usuario es avisado que de entrada a su PIN.

20 El dispositivo 16 de comunicaciones luego manipula el dato de transacción y al identificador de instrumento de transacción financiera encriptado y

PIN, como se describe arriba, y regresa el bloque de dato de transacción asegurado, el identificador de instrumento de transacción financiera encriptado actualizado y el PIN asegurado a través de la red 20 de comunicación al servidor 14.

5 El pago procesado como se describe arriba, en cuyo punto el PIN se valida por el banco.

Se apreciará que a fin de que lo anterior sea implementado en el dispositivo 16 de comunicaciones móviles, el dispositivo se modificará como se describe abajo con referencia a la Figura 5 que ilustra el dispositivo
10 esquemáticamente. La modificación será implementada como varios módulos en el dispositivo 16 de comunicaciones móviles. Estos se pueden implementar como porciones de código identificables, instrucciones computacionales o ejecutables, datos, u objeto computacional para lograr una función, operación, procesamiento o procedimiento particular. Un módulo no necesita implementarse en software solo,
15 pero un módulo se puede implementar en software y/o firmware y/o hardware.

En cualquier caso, el dispositivo de comunicaciones móviles incluye una memoria 34 que tiene almacenadas en la misma una o más claves para usarse para diversos protocolos de comunicación y para descifrar un identificador de instrumento de transacción financiera. La memoria 34 se puede implementar en
20 el propio dispositivo de comunicaciones móviles o puede formar parte de una tarjeta SIM, por ejemplo.

Un módulo de recepción típicamente incorporado en un módulo 36 de comunicaciones móviles se usa para recibir en el dispositivo de comunicaciones móviles un identificador de instrumento de transacción financiera encriptado y un módulo 42 de encriptación/descifrado para descifrar al identificador
5 de instrumento de transacción financiera encriptado.

Una presentación 38 presenta a un usuario del dispositivo de comunicaciones móviles el identificador de instrumento de transacción financiera junto con información relacionada con una transacción financiera.

Un módulo 48 e entrada de datos, por ejemplo, el tablero del
10 dispositivo se usa para recibir el usuario un PIN de autenticación y el módulo 42 de encriptación/descifrado encripta nuevamente cuando menos el identificador de instrumento de transacción financiera y el PIN de autenticación.

Estos luego se transmiten a través de una red de comunicaciones por el módulo 36 de comunicaciones móvil a un servidor para de esta manera
15 instruir al servidor que procese la transacción financiera identificada al usuario.

Se apreciará que los diversos módulos ilustrados en la Figura 5 están adaptados además para llevar a cabo las metodologías arriba descritas.

Se apreciará que esto es solamente un ejemplo de las muchas aplicaciones para las que el presente método y sistema se podría usar.

20 La invención como se ha descrito hasta ahora proporciona una manera nueva y segura de procesar una transacción financiera.

El sistema y método permiten a los usuarios la capacidad de utilizar sus tarjetas expedidas por el banco a través de su dispositivo de comunicaciones móviles. Las tarjetas están registradas y la información está almacenada de manera segura y solamente disponible al usuario del dispositivo 16 de 5 comunicaciones, negando la necesidad de que el cliente tenga la tarjeta física a mano.

10

15

REIVINDICACIONES

1.- Un método para procesar de manera segura una transacción, el método incluyendo:

5 almacenar una pluralidad de identificadores de instrumento de transacción financiera encriptados en una memoria, en donde no hay clave de descifrado para estos almacenados en la memoria y además en donde los identificadores de instrumento de transacción financiera encriptados están cada uno asociados con un dispositivo de comunicaciones móviles;

10 recibir en un servidor una solicitud para procesar una transacción, la solicitud incluyendo una identificación de un dispositivo de comunicaciones móviles;

retirar de la memoria el identificador de instrumento de transacción financiera encriptado asociado con el dispositivo de comunicaciones móviles identificado en la solicitud;

15 transmitir el identificador de instrumento de transacción financiera encriptado retirado al dispositivo de comunicaciones móviles;

recibir del dispositivo de comunicaciones móviles datos de transacción y usar los datos de transacción recibidos para efectuar una transacción financiera.

2.- Un método de conformidad con la reivindicación 1, en donde el dato de transacción recibido del dispositivo de comunicaciones móviles incluye
20 una clave de descifrado para descifrar el identificador de instrumento de

transacción financiera encriptado almacenado, asociado con el dispositivo de comunicaciones móviles.

3.- Un método de conformidad con la reivindicación 1, en donde el dato de transacción recibido del dispositivo de comunicaciones móviles incluye un
5 identificador de instrumento de transacción financiera que se va a usar para efectuar la transacción financiera.

4.- Un método de conformidad con la reivindicación 1, que incluye además la recepción de un PIN del dispositivo de comunicaciones móviles para autorizar una transacción financiera.

10 5.- Un método de conformidad con la reivindicación 4, en donde el PIN es recibido a través de un canal de comunicación diferente al dato de transacción recibido del dispositivo de comunicaciones móviles.

6.- Un método de conformidad con la reivindicación
1, en donde el dato de transacción recibido del dispositivo de comunicaciones
15 móviles incluye uno o más de:

datos de identificación de tercera parte que identificar a una tercera parte a quien se va a pagar una cantidad; y la cantidad que se va a pagar a la tercera parte.

7.- Un método de conformidad con la reivindicación 1, en donde el método comprende además usar el dato de transacción recibido del dispositivo de
20 comunicaciones móvil para crear un paquete de datos de transacción que se va a

transmitir a un sistema financiero que usa el paquete de datos de transacción para efectuar la transacción financiera.

8.- Un método de conformidad con la reivindicación 7, en donde el paquete de datos de transacción está estructurado en el mismo formato que un
5 paquete de datos de presentación de tarjeta de modo que el sistema financiero pueda tratar la transacción financiera como una transacción de presentación de tarjeta.

9.- Un sistema para procesar una transacción, el sistema incluyendo:

una memoria que almacena una pluralidad de identificadores de instrumento de
10 transacción financiera encriptados, en donde no hay clave de descifrado para estos almacenados en la memoria y además en donde los identificadores de instrumento de transacción financiera encriptados están cada uno asociado con un dispositivo de comunicaciones móviles;

un módulo de comunicaciones para recibir una solicitud para procesar una transacción,
15 la solicitud incluyendo una identificación de un dispositivo de comunicaciones móviles;

un módulo de retiro para retirar de la memoria el identificador de instrumento de transacción financiera encriptado asociado con el dispositivo de comunicaciones móviles identificado en la solicitud y para pasar esto al módulo de comunicaciones para transmitirse al dispositivo de comunicaciones móviles; y

20 un módulo de formatear datos en comunicación con el módulo de comunicaciones para recibir del dispositivo de comunicaciones móvil datos de transacción y

para usar los datos de transacción recibidos para efectuar una transacción financiera.

10.- un sistema de conformidad con la reivindicación 9, en donde el módulo de comunicaciones recibe además datos de transacción del dispositivo de
5 comunicaciones móviles, cuyo dato de transacción incluye una clave de descifrado para descifrar un identificador de instrumento de transacción financiera encriptado almacenado, asociado con el
dispositivo de comunicaciones móviles.

11.- Un sistema de conformidad con la reivindicación 9, en donde el
10 módulo de comunicaciones recibe además datos de transacción del dispositivo de comunicaciones móviles, cuyo dato de transacción incluye un identificador de instrumento de transacción financiera que e vfa a usar para efectuar la transacción financiera.

12.- Un sistema de conformidad on la reivindicación 9, en donde el
15 módulo de comunicaciones recibe además un PIN del dispositivo de comunicaciones móviles para autorizar una transacción financiera.

13.- Un sistema de conformidad con la reivindicación 12, en donde el módulo de comunicaciones recibe el PIN a través de un canal de comunicación diferente al dato de transacción recibido del dispositivo de comunicaciones
20 móviles.

14.- Un sistema de conformidad con la reivindicación 10, en donde el dato de transacción recibido del dispositivo de comunicaciones móviles incluye uno o más de:

dato de identificación de tercera parte que identifica a una tercera parte a quien se
5 va a pagar una cantidad, Y la cantidad que se va a pagar a la tercera parte.

15.- Un sistema de conformidad con la reivindicación 10, en donde el módulo para formatear datos usa además el dato de transacción recibido del dispositivo de comunicaciones móvil para crear además un paquete de datos de transacción que se va a transmitir a un sistema financiero que usa el paquete de
10 datos de transacción para efectuar la transacción financiera.

16.- Un sistema de conformidad con la reivindicación 15, en donde el módulo para formatear datos estructura el paquete de datos de transacción en el mismo formato que un paquete de datos de presentación de tarjeta de modo que el sistema financiera puede tratar la transacción financiera como una transacción
15 de presentación de tarjeta.

17.- Un método para procesar de manera segura una transacción, el método incluyendo:

almacenar en el dispositivo de comunicaciones móvil una clave para descifrar un identificador de instrumento de transacción financiera encriptado,
20 recibir en el dispositivo de comunicaciones móvil un identificador de instrumento de transacción financiera encriptado, descifrar el identificador de instrumento de

transacción financiera encriptado,

presentar a un usuario del dispositivo de comunicaciones móvil el identificador de instrumento de transacción financiera junto con información relacionada con una transacción financiera;

- 5 avisar al usuario que de entrada a un PIN de autenticación; encriptar el PIN de autenticación y transmitir este a través de una red de comunicaciones a un servidor para de esta manera instruir al servidor que procese la transacción financiera identificada al usuario.

18.- Un método de conformidad con la reivindicación 17, en donde la
 10 clave para descifrar el identificador de instrumento de transacción financiera encriptado es la misma clave que está almacenada en una memoria en el dispositivo de comunicaciones móvil y usada por el dispositivo de comunicaciones móvil para autenticar comunicaciones a través de la red de comunicaciones móviles.

- 15 19.- Un método de conformidad con la reivindicación 17, en donde el identificador de instrumento de transacción financiera y PIN de autenticación se transmiten a través de diferentes redes de comunicaciones al servidor.

20.- Un dispositivo de comunicaciones móvil que incluye:

una memoria que tiene almacenada en un dispositivo de
 20 comunicaciones móvil una clave para descifrar un identificador de instrumento de transacción financiera encriptada;

un módulo de recepción para recibir en el dispositivo de comunicaciones móviles un identificador de instrumento de transacción financiera encriptado;

un módulo de descifrado para descifrar el identificador de instrumento de transacción financiera encriptado;

una presentación para presentar a un usuario del dispositivo de comunicaciones móviles el identificador de instrumento de transacción financiera junto con información relacionada con una transacción financiera;

un módulo de entrada de dato para recibir del usuario un PIN de autenticación; y

un módulo de encriptación para transmitir el PIN a través de una red de comunicaciones a un servidor para de esta manera instruir al servidor que procese la transacción financiera identificada al usuario.

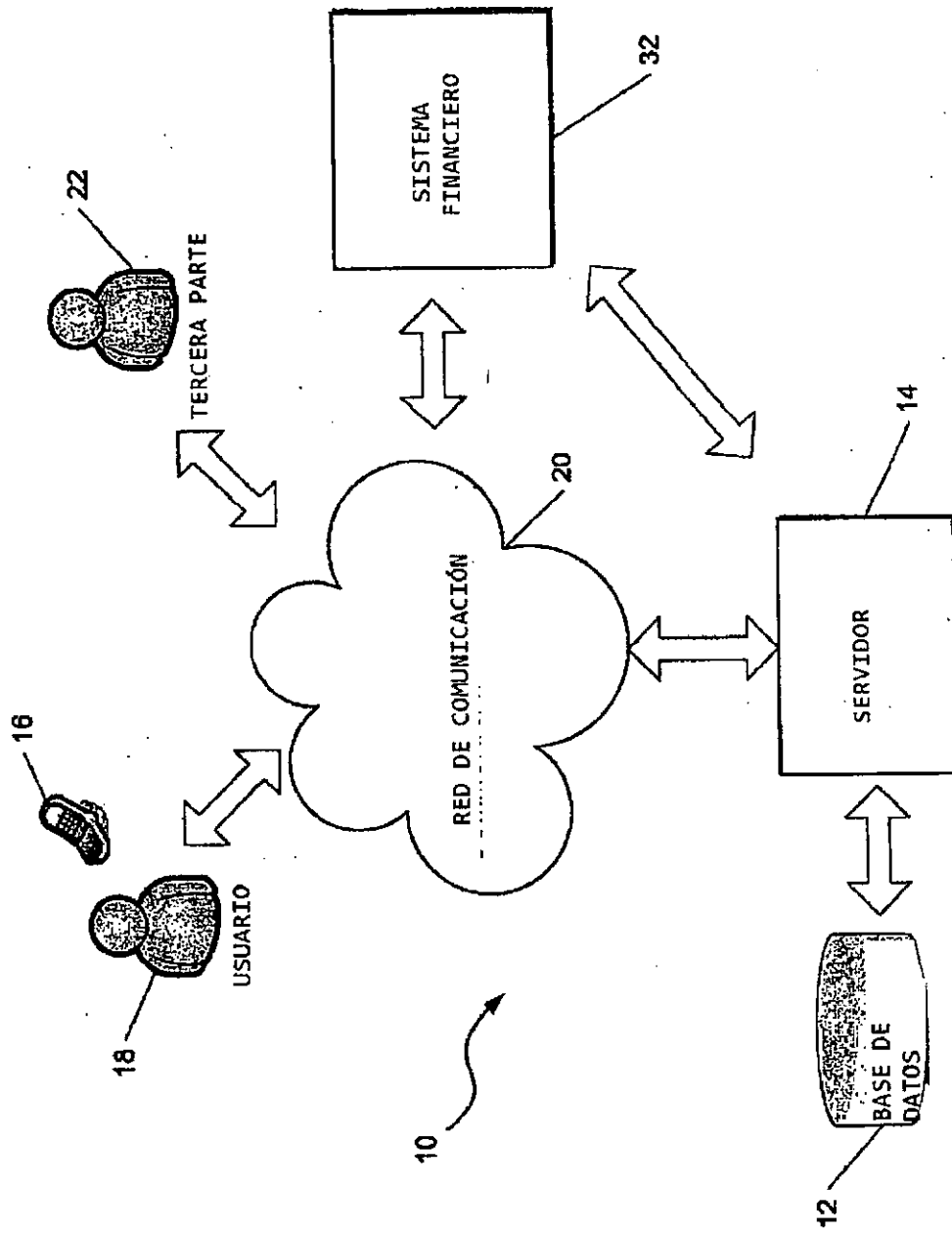


FIGURA 1

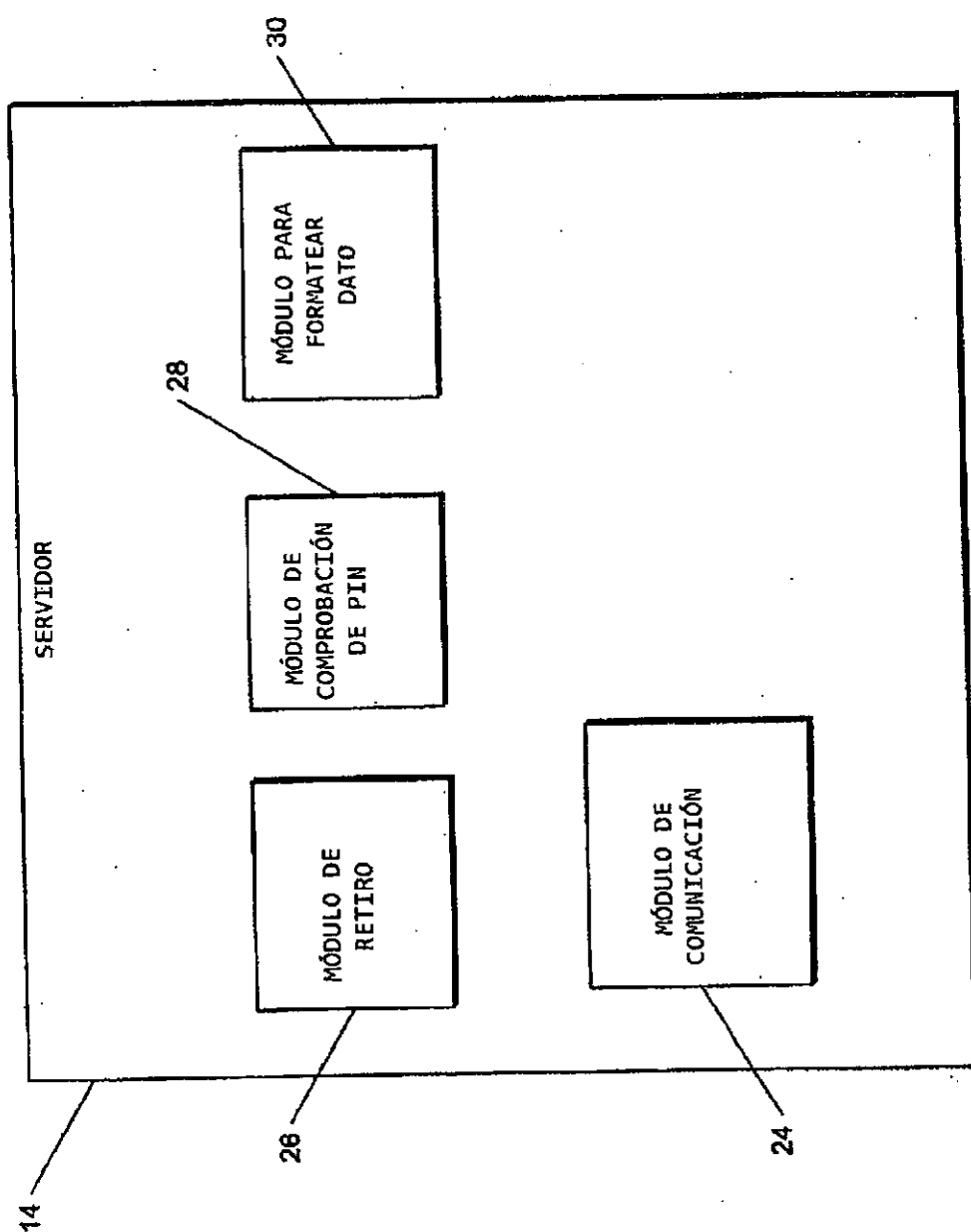


FIGURA 2

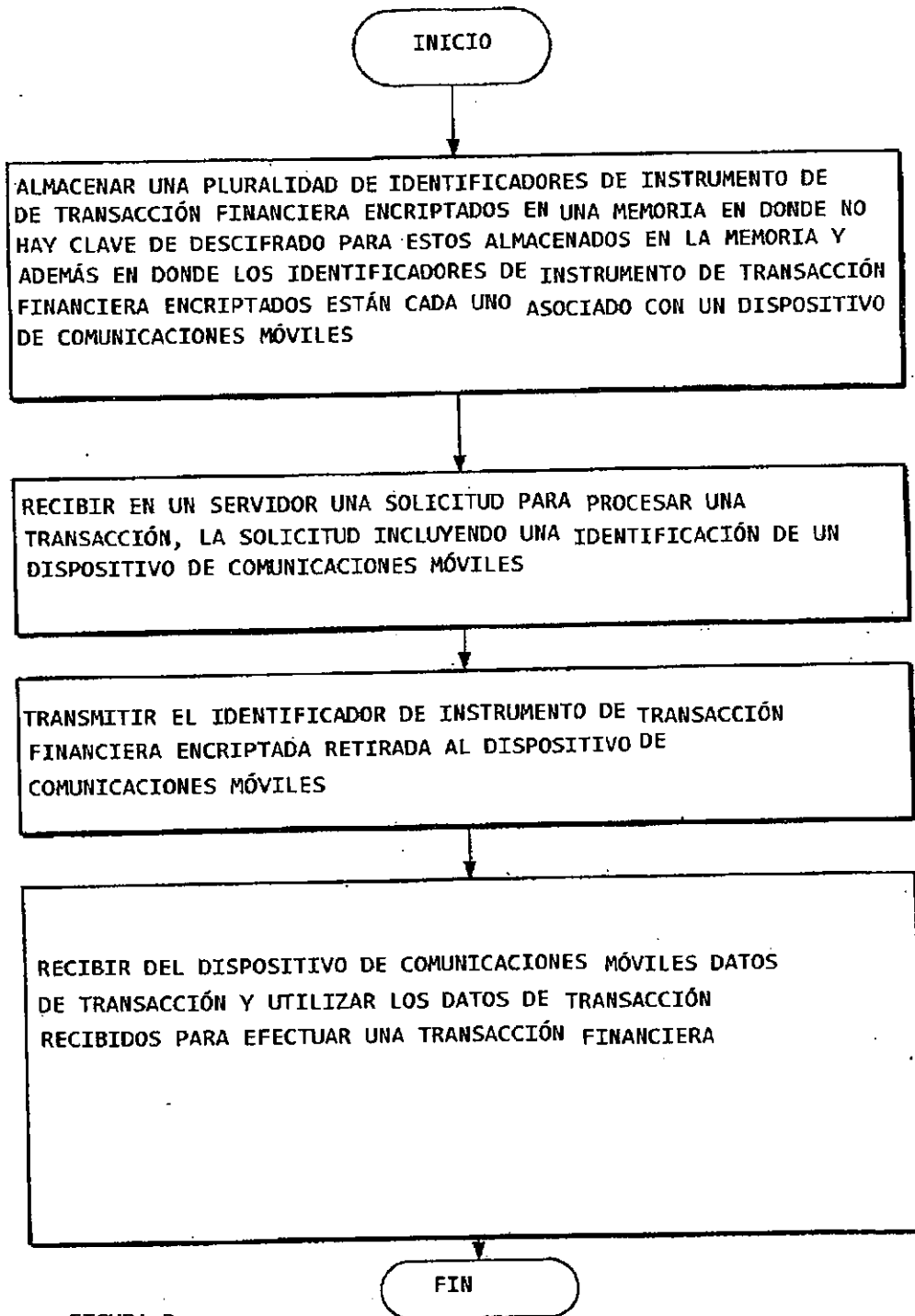


FIGURA 3

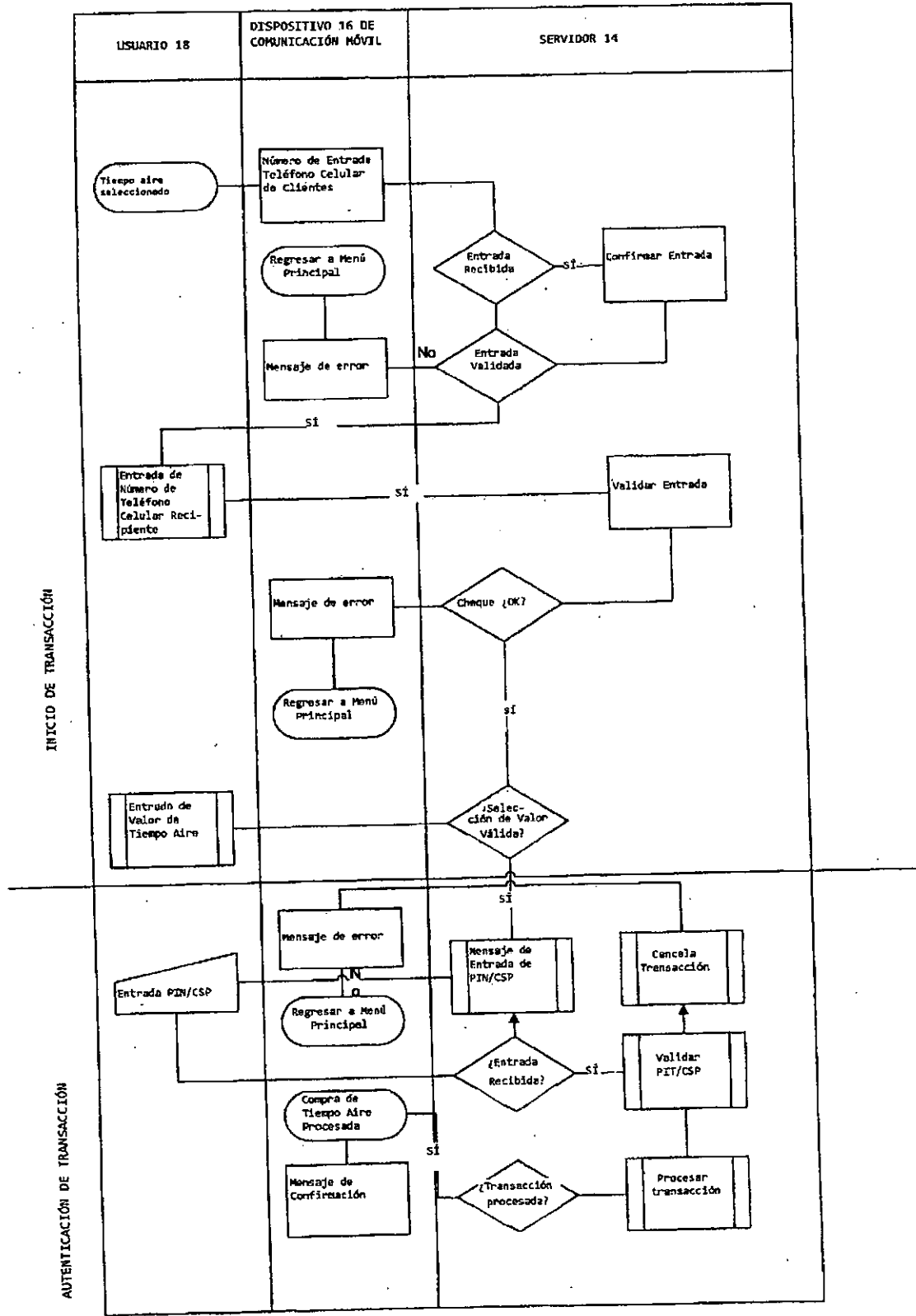


FIGURA 4

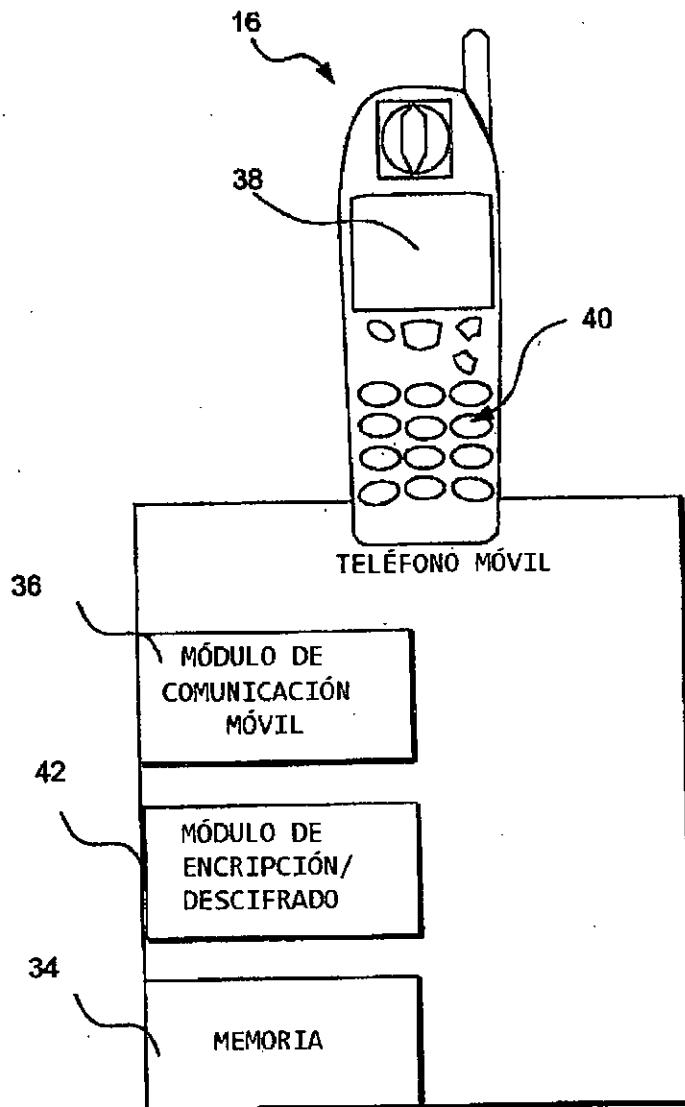


FIGURA 5

PATENTE DE INVENCION ☐ **MODELO DE UTILIDAD** ☐ **Art 33 Decisión 486/00**

☐ Indicación que solicita una patente

☐ Datos de identificación del solicitante o de la persona que presenta la solicitud

☐ Descripción de la invención

☐ Dibujos de ser estos pertinentes

☐ Comprobante de pago de las tasas establecidas (De ser caso formato de descuento)

Completa ☐

Incompleta ☐

PATENTE DE INVENCION PCT ☒ **MODELO DE UTILIDAD PCT** ☐ **Art .33 Decisión 486/00, Circular Única**

1 ☒

Indicación que se solicita una PCT

13 ☒

Copia de la solicitud en español, tal como fue presentada inicialmente (capitulo descriptivo, reivindicatorio, resume)

45 ☒

Dibujos de ser estos pertinentes.

2 ☒

Comprobante de pago de las tasas establecidas (de ser el caso formato de descuento)

Completa ☒

Incompleta ☐

DISEÑO INDUSTRIAL ☐ **(Art. 119 Decisión 486/00)**

☐ Indicación que se solicita Diseño Industrial

☐ Datos de identificación del solicitante o de la persona que presenta la solicitud

☐ Representación gráfica y fotográfica del Diseño industrial o muestra del material que Incorpora el diseño

☐ Comprobante de pago de las tasas establecidas

Completa ☐

Incompleta ☐

ESQUEMA TRAZADO ☐ **(Art. 92 Decisión 486/00)**

☐ Indicación que se solicita un esquema de trazado

☐ Datos de identificación del solicitante o de la persona que presenta la solicitud

☐ Representación grafica de un esquema de trazado

☐ Comprobante de pago de las tasas establecidas

Completa ☐

Incompleta ☐

Bogotá D.C.,
2020

Doctor(a)
LLOREDA RICAURTE ALICIA
Apoderado(a) y/o Representante de
MTN MOBILE MONEY SA (PTY) LTD

REFERENCIA	Radicación No.	11 082169
	Solicitud internacional	PCT/ZA2009/055838
	Fecha inicio fase nacional	23/07/2011
	Trámite	11
	Evento	378
	Actuación	430
	Oficio No.	

E 1 247 J

Como resultado del examen de forma, realizado con fundamento en el artículo 38 de la Decisión 486 de la Comisión de la Comunidad Andina, artículo 27 del Tratado de Cooperación en Materia de Patentes (PCT), regla 51 bis del Reglamento y Circular Única de la Superintendencia de Industria y Comercio, se le comunica que:

1. La solicitud no contiene el poder debidamente otorgado, con el lleno de los requisitos exigidos por los artículos 63 y subsiguientes del Código de Procedimiento Civil. Adicionalmente, deberá presentar el documento que acredita la existencia y representación legal de la sociedad solicitante, cuando ésta fuere persona jurídica.
2. La solicitud no contiene la copia del documento en que consta la cesión del derecho a la patente del inventor al solicitante o a su causante, conforme a lo establecido por el artículo 26 literal k) de la Decisión 486 de la Comisión de la Comunidad Andina. Cuando se trate de documentos otorgados en el extranjero, estos deberán legalizarse de conformidad con lo dispuesto por los artículos 259 y 260 del Código de Procedimiento Civil. Cuando se trate de las declaraciones a que hace referencia la Regla 4.17 ii) del Tratado de Cooperación en Materia de Patentes PCT., el alcance de las tales declaraciones se determinará según indiquen claramente una cesión de derechos del inventor al solicitante o su causante, de conformidad con lo dispuesto en el numeral 5.2.15 del Capítulo Quinto, Título X de la Circular Única de Superintendencia de Industria y Comercio.

En cumplimiento de lo dispuesto por el artículo 39 de la Decisión 486, se le requiere para que dentro del término de dos meses siguientes a la fecha de notificación del presente oficio, complete los requisitos anteriormente enunciados. En caso de no dar cumplimiento al presente requerimiento, la solicitud se considerará abandonada y perderá su prelación.

Continúa en la página siguiente...

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 5.2, literal e), del capítulo quinto del título primero de la Circular Unica No.10 de 2001.



JOSE LUIS SALAZAR LOPEZ
Director de Nuevas Creaciones (C)

11 AGO. 2011

El anterior requerimiento fue notificado por fijación en lista de fecha _____
adpa11

Bogotá D.C.,
2020

Doctor(a)
LLOREDA RICAURTE ALICIA
Apoderado(a) y/o Representante de
MTN MOBILE MONEY SA (PTY) LTD

REFERENCIA	Radicación No.	11 082169
	Solicitud internacional	PCT/ZA2009/055838
	Fecha inicio fase nacional	23/07/2011
	Trámite	11
	Evento	378
	Actuación	430
	Oficio No.	1 247 2

Teniendo en cuenta que el capítulo reivindicatorio presentado excede de diez reivindicaciones, es necesario que cancele la tasa establecida por cada reivindicación adicional presentada, de conformidad con lo dispuesto en la resolución de tasas vigente para la fecha de presentación de la solicitud, so pena de que no sean tenidas en cuenta dentro del presente trámite administrativo.

En consecuencia, con fundamento en lo previsto por el artículo 12 del Código Contencioso Administrativo, se le requiere para que dentro del término de dos (2) meses siguientes a la fecha de notificación del presente oficio atienda el requerimiento aquí señalado. Lo anterior, con el alcance que para tal efecto establece el artículo 13 de la misma codificación, respecto de las reivindicaciones adicionales.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 5.2, literal e), del capítulo quinto del título primero de la Circular Única N° 10 de 2001.



JOSE LUIS SALAZAR LOPEZ
Director de Nuevas Creaciones (C)

1.1 AGO. 2011

El anterior requerimiento fue notificado por fijación en lista de fecha _____.
adpa11