

No. 12-121806- -00000-0000

Fecha: 2012-07-19 13:34:03 Dep. 2020 DIR.NUEVASOR
Tra 2 PATENTES Eve 1 REGDEPOSITO
Act. 411 PRESENTACION Folios: 133

Act. 411 PRESENTACION

Folios 135

Industria y Comercio

SUPERINTENDENCIA

DELEGATURA PROPIEDAD INDUSTRIAL

REGISTRO PATENTE DE INVENCION

EXPEDIENTE No _____

TITULO SISTEMA Y MÉTODO PARA LLEVAR A CABO TRANSACCIONES FINANCIERAS

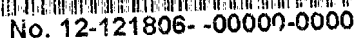
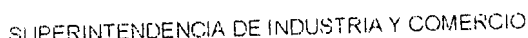
CLASIFICACION INTERNACIONAL _____

SOLICITANTE PLATAMOVIL INTERNATIONAL BV

DOMICILIO CURACAO, ANTILLAS HOLANDESAS

APODERADO DARIO CARDENAS NAVAS

BOGOTA D.C. _____



Fecha: 2012-07-19 13:34:03 Dep 2020 DIR NIEVASCR
Tra. 2 PATENTES Eve: 1 REGDEPOSITO
Act. 411 PRESENTACION Folios: 133
Act. 411 PRESENTACION Folios: (135)

1

X

Patente de Modelo de Utilidad

2

IDENTIFICACION

☐ NIT

☒ Otro

Número

3

IDENTIFICACIÓN

☐ NIT☐ Otro

Número 17066629 Bta	TP	1250
---------------------	----	------

En caso de haber presentado poder general para asuntos que se adelanten ante la Delegatura de Propiedad Industrial, sírvase indicar el número de radicación (del poder)

4

Nombre : (Ver adjunto)
Dirección: (Ver adjunto)
Nacionalidad o Domicilio: (Ver adjunto)

5

SISTEMA Y MÉTODO PARA LA REALIZACIÓN DE TRANSACCIONES FINANCIERAS

VEINTE (20)

7

(33) País de Origen

(32) Fecha

(31) Número de Solicitud

Prioridad

US

25.08.2011

13/217,634

X

SI

NO

9 Para publicar a partir de la fecha de la presente solicitud o de la prioridad invocada a los:

☐ Inmediato

6 meses

12 meses

18 meses

Comprobante de Pago No:

12-0063919

Fecha:

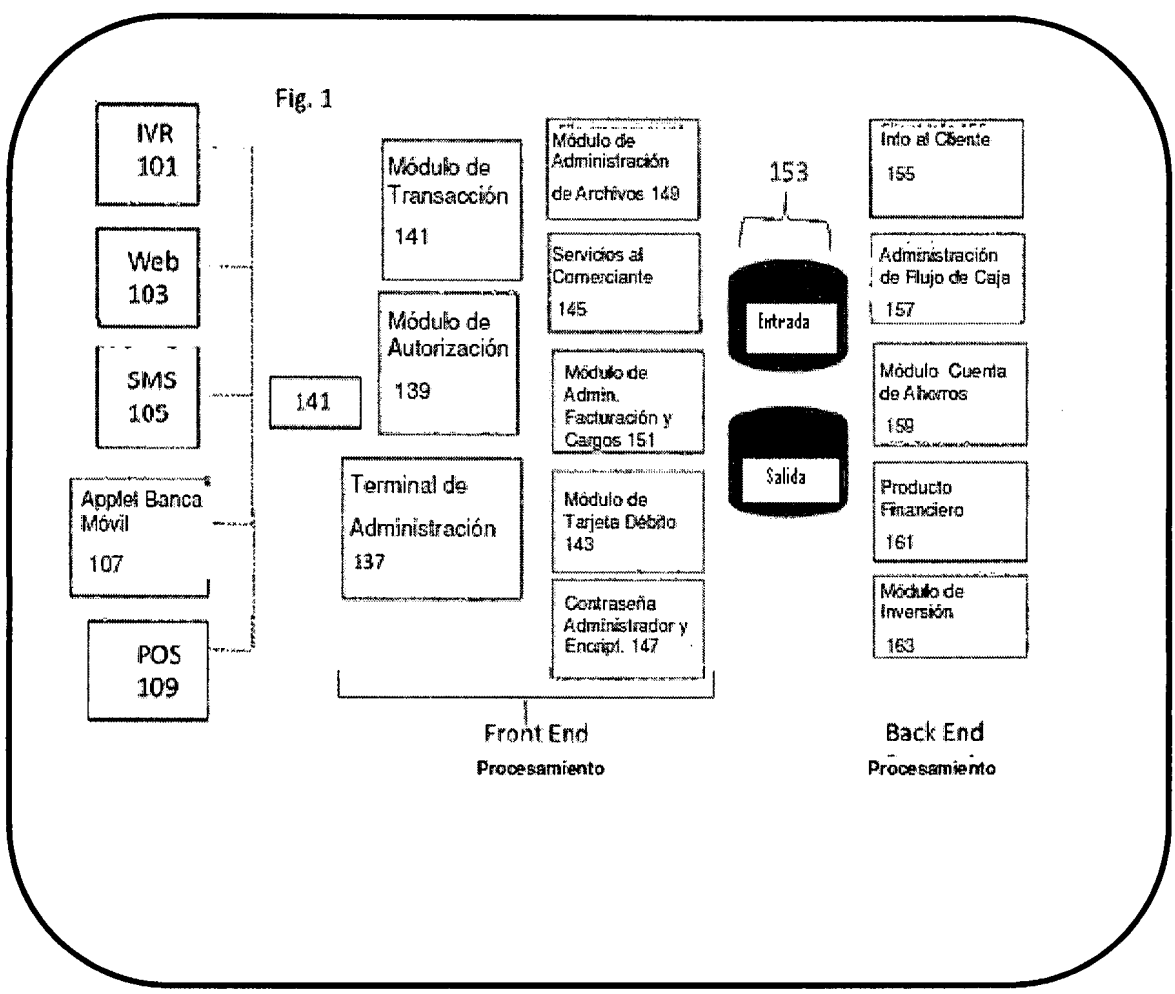
25.06.2012

11

SISTEMA Y MÉTODO PARA LLEVAR A CABO TRANSACCIONES FINANCIERAS

- ☒ X
- Comprobante de pago de la tasa de presentación de la solicitud
- ☐
- Comprobante de pago de la tasa por concepto de excedente de palabras en la publicación
- ☒ X
- Comprobante de pago por reivindicación de prioridad
- ☐
- Documento que acredita la existencia y representación legal de la persona jurídica peticionaria, en Cuanto no estén inscritas en alguna Cámara de Comercio Colombiana.
- ☐
- Poder, si fuere el caso
- ☐
- Certificado de la fecha de presentación de la solicitud prioridad expedida por la autoridad correspondiente y una copia certificada de la primera solicitud, si se reivindica prioridad.
- ☒ X
- Traducción simple de la primera solicitud, si se reivindica prioridad.
- ☒ X
- Documento de cesión del inventor al solicitante o a su causante.
- ☒ X
- Resumen
- ☒ X
- Descripción de la invención
- ☒ X
- Una o más reivindicaciones
- ☒ X
- Dibujos y/o planos necesarios
- ☐
- 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
- ☐
- De ser el caso, certificado de depósito del material biológico
- ☒ X
- Arte final 12 x 12 cm
- ☐
- De ser el caso, información sobre otras solicitudes de patente o títulos obtenidos en el extranjero por El mismo titular o su causante, relacionadas parcial o totalmente con la invención de esta solicitud.

12 FIGURA CARACTERÍSTICA



13 Solicito la concesión de la patente,

NOMBRE: DARIO CARDENAS NAVAS

FIRMA:

C.C.17066629 BTA

TP 1250 CSJ

SISTEMA Y MÉTODO PARA LLEVAR A CABO TRANSACCIONES FINANCIERAS	
INVENTOR	Nombre : FEDERICO L. FUENTES
	Dirección: 3640 YACHT CLUB #410, AVENTURA, FLORIDA 33180, ESTADOS UNIDOS DE AMERICA
	Nacionalidad o Domicilio: VENEZOLANO
INVENTOR	Nombre : RICARDO A. ESPAÑA
	Dirección: AV. PERIMETRAL URB LOS CASTORES, MIRANDA, VENEZUELA
	Nacionalidad o Domicilio: VENEZOLANO
INVENTOR	Nombre : CARLOS E. CONVIT
	Dirección: AV. MANUEL FELIPE TOVAR, SAN BERNARDINO, CARACAS, VENEZUELA
	Nacionalidad o Domicilio: VENEZOLANO

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
NIT : 800.176.089-2
- / -

Industria y Comercio SUPERINTENDENCIA	RECIBO DE CAJA	No. 12 - 0063919
		Bogotá D.C., Junio 25 de 2012 - 12:29:15

RECIBIDO DE : CARDENAS & CARDENAS ABOGADOS PI LTDA NI 830.083.491

*** Soporte del Pago ***

TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	VR PAGO
CONSIGNACION	BANCO DE BOGOTA	062754387	196860112	25/06/2012	9.610.000.00

*** Conceptos Pagados ***

CANT.	RENTISTICO	CONCEPTO	Vr. UNIDITARIO	Vr. CONCEPTO
1	50005-01-01 SOLICITUDES	1 TRAMITES DE SOL. DE PATENTE DE INVENCIÓN	590.000.00	590.000.00
				\$590.000.00

SON: **QUINIENTOS NOVENTA MIL PESOS MONEDA CORRIENTE***

Responsable: _____
Recibo de Caja Aplicado al Expediente No. _____

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

No. 12-121806-00000-0000
Fecha 2012-07-19 13:34:03 Dep. 2020 DIR.NUEVASCR
Tra. 2 PATENTES Eve. 1 REGDEPOSITO
Act. 411 PRESENTACION Folios. 133
Act. 411 PRESENTACION Folios. 135

CARDENAS & CARDENAS
ABOGADOS

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO NIT : 800.176.089-2 - / -					
Industria y Comercio SUPERINTENDENCIA	RECIBO DE CAJA			No. 12 - 0063920	
				Bogotá D.C., Junio 25 de 2012 - 12:29:15	
RECIBIDO DE : CARDENAS & CARDENAS ABOGADOS PI LTDA				NI 830.083.491	
*** Soporte del Pago ***					
TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	VR. PAGO
CONSIGNACION	BANCO DE BOGOTA	062754387	196860112	25/06/2012	9.610.000.00
*** Conceptos Pagados ***					
CANT. RENTISTICO	CONCEPTO			Vr. UNIDITARIO	Vr. CONCEPTO
10 50005-01-01 SOLICITUDES	1607 REIVINDICACION UNITARIA ADICIONAL A LAS 10 INICIALES			30.000.00	300.000.00
					\$300.000.00
=====					
SON: **TRESCIENTOS MIL PESOS MONEDA CORRIENTE***					
Responsable: _____					
Recibo de Caja Aplicado al Expediente No. _____					
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO					
					
No. 12-121806- -00000-0000					
Fecha: 2012-07-19 13:34:03 Dep. 2020 DIR NUEVASOR					
Tra. 2 PATENTES Eve: 1 REGDEPOSITO					
Act. 411 PRESENTACION Folios: 133					
Act. 411 PRESENTACION Folios: 135					
CARDENAS & CARDENAS ABOGADOS					
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					
Junio 25 de 2012 - 12:29:17					

	SUPERINTENDENCIA DE INDUSTRIA Y.COMERCIO										6
	DIVISION DE NUEVAS CREACIONES										
	TARJETA DE ARCHIVO PROPIETARIOS										
	PATENTE DE INVENCION		X	PCT		MODELO DE UTILIDAD			DISEÑO INDUSTRIAL		
(21) No de solicitud:				(22) Fecha de solicitud:							
(51) Clasificación Internacional:											
(71)Solicitante(s) PLATAMOVIL INTERNATIONAL B.V.											
(72) Inventor(es) 1. Federico L. Fuentes 2. Ricardo A. España 3. Carlos E. Convit											
(74) Apoderado: DARIO CARDENAS NAVAS											
(30) Prioridad		(31) No Prioridad		(32) Fecha		(33) País					
		13/217,634		25.08.2011		US					
(85) Fecha inicio fase nacional:											
(86) Datos relativos a la presentación de la solicitud PCT Fecha de presentación de la solicitud: No de solicitud:											
(54) Título SISTEMA Y MÉTODO PARA LA REALIZACIÓN DE TRANSACCIONES FINANCIERAS											

	EXTRACTO PARA PUBLICACIÓN ☒ Patente de Invención ☐ Patente modelo de utilidad ☐ PCT
---	--

(21) No De solicitud	(51) int. Cl:
(22) Fecha de solicitud	(71) Solicitante (s) PLATAMOVIL INTERNATIONAL B.V.
(30) Prioridad (31) No Prioridad 13/217,634 (32) Fecha 25.08.2011 (33) País US	(72) Inventor(es) 1. Federico L. Fuentes 2. Ricardo A. España 3. Carlos E. Convit
(74) Apoderado (s) DARIO CARDENAS NAVAS	
(54) Título SISTEMA Y MÉTODO PARA LA REALIZACIÓN DE TRANSACCIONES FINANCIERAS	
Las casillas identificadas con 85, 86 y 87 sólo aplican para PCT	
(85) Fecha límite de inicio Fase Nacional (86) Datos relativos a la presentación de la solicitud PCT Fecha de presentación de la solicitud No de Solicitud PCT	(87) Publicación internacional Fecha No Publicación

Resumen reivindicación (es):
Los sistemas y métodos de la presente invención incluyen una arquitectura de sistema integral que permite el acceso a instituciones financieras no bancarias (NFBIs) y bancos a través de dispositivos en punto de venta y teléfonos móviles, por ejemplo. La presente invención involucra el uso de un estándar ISO 8583 modificado para permitir a los usuarios hacer interfase con un sistema de procesamiento de front end directamente desde los dispositivos no tradicionales. La presente invención también permite banca móvil con los NBFi a través del uso de una aplicación que reside en un teléfono móvil de un usuario, que permite el encapsulamiento de información del usuario como XML, por ejemplo, y la transmisión de ellos sobre http mientras cumple con el estándar ISO 8583, y además permite la encriptación de ciertos datos de usuario, sin que tenga que recurrir al acceso a la página web de banca móvil. En un aspecto de la invención, una aplicación POS puede ejecutarse en la parte superior de PCI para permitir a los usuarios hacer compras utilizando fondos pre-depositados en una cuenta NBFi.

9

DOCKET NO.: 1496.PLAT0002U

ASSIGNMENT

WHEREAS, we, Federico L. Fuentes, a citizen of Venezuela, residing at 3640 Yacht Club Drive #410, Aventura, Florida 33180; Ricardo A. España, a citizen of Venezuela, residing at Av. Perimetral Urb Los Castores, Edif. El Centro P.2 Apto 2-B, Apartamento 1204, San Antonio de Los Altos Edo Miranda, Venezuela; and Carlos E. Convit, a citizen of Venezuela, residing at Av. Manuel Felipe Tovar Edif. Palmali Apto 6-C Piso 6, San Bernardino, Caracas, Venezuela, hereinafter referred to as the assignors, are the joint inventors of certain inventions or improvements for which we have made application for Letters Patent to the United States, identified as U.S. Patent Application No. 13/217,634 filed August 25, 2011, entitled SYSTEM AND METHOD FOR CONDUCTING FINANCIAL TRANSACTIONS; and

WHEREAS, Platamovil International BV., hereinafter referred to as the assignee, of Kaya W.F.G. (Jombi) Mensing 36, Curacao, a corporation of Curacao, is desirous of acquiring the entire right, title and interest in and to the said inventions or improvements and in and to the said application, and in, to and under any and all Letters Patent which may be granted on or as a result thereof in any and all countries.

NOW, THEREFORE, for good and valuable consideration, the receipt of which is hereby acknowledged, and intending to be legally bound hereby, we, the said assignors, have sold, assigned, transferred and set over, and by these presents do hereby sell, assign, transfer and set over to said assignee, the entire right, title and interest in and to said inventions or improvements and said application and any and all continuations, divisions and renewals of and substitutes for said application, and in, to and under any and all Letters Patent which may be granted on or as a result thereof in the United States and any and all other countries, and any reissue or reissues or extension or extensions of said Letters Patent, including the full right to sue for and collect damages for past violations of provisional rights having arisen from any publication of said application or any continuations, divisions, or renewals of or substitutes for said application. We further assign to and authorize said assignee, to file in our names applications for Letters Patent in all countries, the same to be held and enjoyed by said assignee, its successors, assigns, nominees or legal representatives, to the full end of the term or terms for which said Letters Patent respectively may be granted, reissued or extended, as fully and entirely as the same would have been held and enjoyed by us had this assignment, sale and transfer not been made.

AND we hereby covenant that we have full right to convey the entire interest herein assigned, and that we have not executed and will not execute any agreement in conflict herewith, and we further covenant and agree that we will each time request is made and without undue delay, execute and deliver all such papers as may be necessary or desirable to perfect the title to said inventions or improvements, said application and said Letters Patent to said assignee, its successors, assigns, nominees, or legal representatives, and each of us agrees to communicate to said assignee or to its nominee all known facts respecting said inventions or improvements, said application and said Letters Patent, to testify in any legal proceedings, to sign all lawful papers, to execute all disclaimers and divisional, continuing, reissue and foreign applications, to make all rightful oaths, and generally to do everything possible to aid said assignee, its

DOCKET NO.: 1496.PLAT0002U

successors, assigns, nominees and legal representatives to obtain and enforce for its or their own benefit proper patent protection for said inventions or improvements in any and all countries.

AND we hereby authorize and request the Commissioner of Patents and Trademarks of the United States and any official of any country or countries foreign to the United States whose duty it is to issue patents on applications as aforesaid, to issue to said assignee, as assignee of the entire right, title and interest, any and all Letters Patent for said inventions or improvements, including any and all Letters Patent of the United States which may be issued and granted on or as a result of the application aforesaid, in accordance with the terms of this assignment.

AND this Assignment may be executed in multiple counterparts, each of which shall be deemed to be an original of this Assignment. Additionally, we hereby authorize our attorneys to collect the signature pages of each executed counterpart and to attach those signature pages to a single copy of this instrument, which single copy and attached signature pages together shall constitute an original of this Assignment.

IN WITNESS WHEREOF, we have hereunto set our hands and seals.

8/23/2011
Date



Federico L. Fuentes (L.S.)

8/22/2011
Date



Ricardo A. España (L.S.)

8/25/2011
Date



Carlos E. Convit (L.S.)

CESION

CONSIDERANDO QUE, nosotros, Federico L. Fuentes, un ciudadano de Venezuela, residente en 3640 Yacht Club Drive #410, Aventura, Florida 33180; Ricardo A. España, un ciudadano de Venezuela, residente en Ac. Perimetral Urb. Los Castores, Edif. El Centro P.2 Apto 2-B, Apartamento 1204, San Antonio de Los Altos Edo Miranda, Venezuela; y Carlos E. Convit, un ciudadano de Venezuela, residente en Av. Manuel Felipe Tovar Edif. Palmali Apto 6-C Piso 6, San Bernardino, Caracas, Venezuela, en adelante denominados los cedentes, somos los inventores conjuntos de ciertas invenciones o mejoras para las cuales hemos efectuado solicitud de Título de Patente de los Estados Unidos, identificada como la Solicitud de Patente de los Estados Unidos No. 13/217,634 presentada en Agosto 25, 2011, titulada SISTEMA Y METODO PARA LA REALIZACION DE TRANSACCIONES FINANCIERAS; y

CONSIDERANDO QUE, Platamovil International BV., en adelante denominada como el cesionario, de Kaya W.F.G. (Jombi) Mensing 36, Curacao, una empresa de Curacao, tiene el deseo de adquirir la totalidad del derecho, título e interés en y para las mencionadas invenciones o mejoras, y en y para la mencionada solicitud, y en, para y bajo cualesquiera y todos los Títulos de Patente que puedan ser otorgados en o como resultado del mismo en cualquiera y todos los países.

EN CONSECUENCIA, como contraprestación a título oneroso, cuyo recibo y reconocimiento se acusa mediante el presente, y con la intención de estar legalmente sometido a este, nosotros, los mencionados cedentes, hemos vendido, cedido, transferido, y entregado, y por la presente, vendemos, cedemos, transferimos, y entregamos al mencionado cesionario, la totalidad del derecho, título e interés en y para las mencionadas invenciones o mejoras y la solicitud mencionada, y en, para y bajo todas las continuaciones, divisiones y renovaciones de y sustitutas de la solicitud mencionada y en, para y bajo todos

los Títulos de Patente que puedan ser otorgados en o como resultado del mismo en los Estados Unidos y cualquiera y todos los demás países, y cualquier reemisión o reemisiones o extensión o extensiones de los Títulos de Patentes mencionados, incluyendo la totalidad del derecho para demandar por y cobrar daños y perjuicios por violaciones pasadas de derechos provisionales que se hayan originado de cualquier publicación de la solicitud mencionada o cualesquiera continuaciones, divisiones, o renovaciones de o sustitutas para la solicitud mencionada. Además cedemos y autorizamos a dicho cesionario, a presentar en nuestros nombres solicitudes para Títulos de Patente en todos los países, el mismo para que se obtenga y disfrute por los cesionarios mencionados, sus sucesores, cesionarios, nominados o representantes legales, hasta la totalidad del término o términos para el cual los mencionados Títulos de Patente puedan ser otorgados, reemitidos o extendidos, respectivamente, de la forma más completa y total como la misma pudiera haber sido detentada y disfrutada por nosotros teniendo esta cesión, venta y transferencia si no se hubiere efectuado.

Y por medio de la presente acordamos que tenemos el derecho total para transmitir la totalidad del interés cedido por el presente, y que no hemos firmado y no firmaremos cualquier acuerdo en conflicto con el presente y además pactamos y acordamos que cada vez que se realice una solicitud y sin un retraso injustificado firmaremos y entregaremos todos los documentos que puedan ser necesarios o deseables para perfeccionar el título de los inventos o mejoras mencionadas, dicha solicitud y dichos Títulos de Patente para el cesionario mencionado, sus sucesores, cesionarios, nominados, o representantes legales, y cada uno de nosotros acordamos comunicar al cesionario mencionado o a su nominado todos los hechos conocidos respecto de dichas invenciones o mejoras, dicha solicitud y dichos Títulos de Patente, para testificar en cualesquiera procedimientos legales, para firmar señalar todos los documentos legales, para firmar todas las exenciones de responsabilidad y solicitudes divisionales, continuadas, reemitidas y extranjeras, para hacer los juramentos legítimos, y en general hacer todo lo posible para ayudar a tal cesionario, sus sucesores, cesionarios, nominados y representantes legales para obtener y hacer cumplir para su propio beneficio la

protección de patente apropiada para las invenciones o mejoras mencionadas en cualquiera y todos los países.

Y por la presente autorizamos y solicitamos al Comisionado de Patentes y Marcas de los Estados Unidos y cualquier funcionario de cualquier país o países extranjeros a los Estados Unidos cuya obligación sea la de emitir patentes en solicitudes como las mencionadas emitir a los mencionados cesionarios, como cesionarios de la totalidad del derecho, título e interés, y cualquiera y todos los Títulos de Patente para las mencionadas invenciones o mejoras, incluyendo cualesquiera y todos los Títulos de Patente de los Estados Unidos que puedan ser emitidos y otorgados en o como resultado de la solicitud anteriormente mencionada, de acuerdo con los términos de esta cesión.

Y esta Cesión puede ser firmada en múltiples ejemplares, cada uno de los cuales será estimado como un original de esta Cesión. Adicionalmente, autorizamos por la presente a nuestros abogados para recoger la página de firmas de cada ejemplar firmado y para adjuntar esas páginas de firmas a una única copia de este instrumento, cuyas copias únicas y páginas de firmas adjuntas constituirán juntas un original de esta Cesión.

EN FE DE LO CUAL, suscribimos el presente con nuestras firmas y sellos.

8/23/2011
Date



Federico L. Fuentes (L.S.)

8/22/2011
Date



Ricardo A. España (L.S.)

8/25/2011
Date



Carlos E. Convit (L.S.)

SISTEMA Y METODO PARA LA REALIZACION DE TRANSACCIONES FINANCIERAS

CAMPO DE LA INVENCION

[0001] La presente invención está relacionada con los sistemas de procesamiento de datos y métodos para la realización de transacciones financieras en una red. En particular, la presente invención se refiere a los sistemas y métodos integrados que suministran un acceso seguro a capital y que permiten transacciones financieras por medio del uso de tecnología inalámbrica, tal como dispositivos móviles.

ANTECEDENTES DE LA INVENCION

[0002] Los negocios dedicados al cambio de cheques y pago de facturas en nombre de otros se esmeran en los Estados Unidos así como en otras partes del mundo. Las familias de bajos ingresos están prácticamente forzadas a utilizar estos servicios debido a los altos honorarios cobrados por los bancos por mantener un saldo bajo en una cuenta y debido a los requisitos de altos depósitos iniciales para abrir una cuenta. Los trabajadores migrantes también se ven obligados a utilizar estos servicios puesto que los bancos no permiten a una persona abrir una cuenta sin que suministre una dirección en los Estados Unidos. En general, un gran porcentaje de la población en los Estados Unidos no tiene acceso a capital o servicios financieros a través de los bancos. Esto es algo que las compañías de cambio de cheques aprovechan al hacer préstamos de corto plazo a un interés muy alto. Estas condiciones han creado un problema que esencialmente, pone en peligro la seguridad de las personas que siempre llevan dinero en efectivo. Estas condiciones también crean un problema potencial ya que pueden afectar la capacidad de una autoridad fiscal para recaudar los impuestos sobre transacciones que no pueden ser rastreadas.

[0003] Las instituciones financieras no bancarias ("NBFIs" – por sus siglas en inglés) se han convertido en una alternativa eficiente para los bancos en términos de suministrar servicios financieros a personas con un patrimonio o recursos económicos limitados. El servicio de aceptación de depósitos monetarios del público está típicamente regulado o controlado por el estado o la ley y las regulaciones federales y estas NBFIs no están exentas de tales leyes o reglamentos. A nivel global, estas NBFIs permiten un acceso más amplio a los

servicios financieros, especialmente a las personas que residen lejos de las grandes ciudades. De hecho, uno de los principales aspectos que limitan la facilidad de acceso a bancos alrededor del mundo es la escasez de sucursales que ofrecen servicios al cliente, etc. No sorprende que uno de los objetivos de las NBFIs sea incrementar el número de lugares donde los clientes pueden ser atendidos por medio del incremento en el número de canales no tradicionales, que autorizan a las instituciones bancarias a ofrecer servicios financieros a través de las NBFIs, tales como tiendas, supermercados, etc. Aunque, las NBFIs constituyen una herramienta contra la exclusión financiera, aún persiste una necesidad de un sistema que permita tener un acceso más fácil a capital o a los servicios financieros a través de las NBFIs y los bancos.

RESUMEN DE LA INVENCION

[0004] A continuación se presenta un resumen simplificado de la invención con el fin de suministrar un entendimiento básico de algunos aspectos de la invención. Este resumen no es una descripción amplia de la invención. No pretende identificar ni elementos clave ni críticos de la invención ni delimitar el alcance de la invención. Su único propósito es presentar algunos conceptos de la invención en una forma simplificada como un preludio a la descripción más detallada que será presentada más adelante.

[0005] La presente invención incluye una arquitectura de un sistema integral que permite el acceso a las NBFIs (o bancos) a través de, por ejemplo, dispositivos de punto de venta y de teléfonos móviles. En una incorporación de la presente invención, el estándar ISO 8583 ha sido ampliado con el fin de permitir a los usuarios una interfase con un sistema de procesamiento front end (que interactúa con los usuarios) directamente desde dispositivos no tradicionales.

[0006] En otra incorporación de la presente invención, la banca móvil con las NBFIs o los bancos puede ser lograda a través del uso de una aplicación que resida en el teléfono móvil de un usuario, que permita el encapsulamiento de la información del usuario como XML, por ejemplo, y la transmisión de aquellas sobre http mientras cumplan con la expansión del anteriormente mencionado ISO 8583, y además permita la encriptación de ciertos datos del usuario. En otra incorporación de la presente invención, una aplicación POS puede ser ejecutada

sobre el estándar PCI para permitir a los usuarios hacer compras utilizando fondos depositados previamente en una cuenta NBFÍ. Para lograr esto, la aplicación POS puede iniciar una sesión con la NBFÍ o el banco y utilizar un mensaje encriptado obtenido a través de tal primera sesión para encriptar información como parte de una segunda sesión que entonces será utilizada para finalizar la transacción mientras la primera sesión expira.

[0007] La siguiente descripción y los dibujos anexos establecen en detalle ciertos aspectos ilustrativos de la invención. Estos aspectos son indicativos, sin embargo, de solo unos pocos de los diversos modos en los cuales los principios de la invención pueden ser empleados y la presente invención está destinada a incluir la totalidad de tales aspectos y sus equivalentes. Otras ventajas y características novedosas de la invención se harán evidentes de la siguiente descripción detallada de la invención cuando sean consideradas en conjunto con los dibujos.

BREVE DESCRIPCION DE LOS DIBUJOS

[0008] La Fig. 1 ilustra una arquitectura de una transacción financiera de acuerdo con una incorporación de la presente invención;

[0009] La Fig. 2 ilustra un método para la creación de una cuenta de usuario de acuerdo con una incorporación de la presente invención;

[0010] La Fig. 3 ilustra un método para transferencia electrónica de efectivo a otra cuenta de acuerdo con una incorporación de la presente invención;

[0011] La Fig. 4 ilustra un método para obtener el uso de un PIN de uso por una sola vez para que sea utilizado en un ATM de acuerdo con una incorporación de la presente invención;

[0012] La Fig. 5 ilustra un método para el procesamiento electrónico de retiro de efectivo a través del uso de POS de acuerdo con una incorporación de la presente invención;

[0013] La Fig. 6 ilustra un método para procesamiento electrónico de compras en el sitio de un comerciante de acuerdo con una incorporación de la presente invención;

[0014] La Fig. 7 ilustra un método para procesamiento electrónico de desembolsos de nómina de acuerdo con una primera incorporación de la presente invención;

[0015] La Fig. 8 ilustra un método para procesamiento electrónico de pagos a beneficiarios de acuerdo con una segunda incorporación de la presente invención; y

[0016] La Fig. 9 ilustra un flujo de transacciones relacionadas con el procesamiento electrónico de compras o retiros de efectivo de acuerdo con una incorporación de la presente invención.

DESCRIPCION DETALLADA DE LAS INCORPORACIONES ILUSTRATIVAS

[0017] La presente invención de ahora en adelante será descrita de forma más completa con referencia a los dibujos que la acompañan, en la cual serán mostradas las incorporaciones preferidas de la invención. Esta invención puede, sin embargo, ser incorporada de muchas formas diferentes y no debiera ser interpretada de una forma limitada a las incorporaciones establecidas en la presente. Más bien, estas incorporaciones se suministran de forma tal que esta divulgación sea exhaustiva y completa, y transmita plenamente el alcance de la invención para los expertos en la técnica.

[0018] Como se podrá apreciar por aquellos expertos en la técnica, porciones de la presente invención pueden ser incorporadas como un método, sistema de procesamiento de datos, o un producto de programa de computador. En consecuencia, estas porciones de la presente invención pueden tomar la forma de una incorporación total de hardware, una incorporación total de software, o una incorporación que combine aspectos de software y hardware. Además, porciones de la presente invención pueden ser implementadas como un producto de programa de computador en un medio de almacenamiento utilizable de un computador que tiene un código de programa legible por computador en el medio. Cualquier medio legible por computador adecuado se puede utilizar incluyendo, pero no limitado a, dispositivos de almacenamiento estáticos y dinámicos, discos duros, dispositivos ópticos de almacenamiento, y dispositivos de almacenamiento magnético.

[0019] La presente invención está descrita a continuación con referencia a ilustraciones de métodos, sistemas, y productos de programa de computador de acuerdo con las incorporaciones de la invención. Se entenderá que los bloques de las ilustraciones, y combinaciones de bloques en las ilustraciones, pueden ser implementadas por instrucciones de programa de computador, dispositivos de hardware, o una combinación de ambos. Estas instrucciones de programa de computador pueden ser suministradas a un procesador de un computador de uso general, computador de uso específico, u otro dispositivo de procesamiento de datos programable para producir una máquina en particular, de tal manera que las instrucciones, que se ejecutan a través del procesador del computador u otro dispositivo programable de procesamiento de datos, implemente las funciones especificadas en el bloque o los bloques.

Transacciones Implementadas Mediante ISO 8583 Modificado

[0020] La Fig. 1 ilustra una arquitectura que ejemplifica el sistema de la presente invención de acuerdo con una incorporación. El sistema incluye un número de módulos de procesamiento front end en interfase con dispositivos remotos a través de una interfase de mensajes ISO 8583, 141 modificada de acuerdo con la presente invención. Aunque el ISO 8583 define un estándar común, no es típicamente utilizada por sistemas o redes transaccionales financieras. En cambio, cada red adapta el estándar para su propio uso con campos personalizados y usos personalizados.

[0021] La colocación de los campos en diferentes versiones del estándar varía. Por ejemplo, los elementos de moneda de las versiones de 1987 y 1993 del estándar ISO 8583 ya no se utilizan en la versión 2003, que tiene al tipo de moneda como un subelemento de cualquier elemento de importe financiero. Al momento de este escrito, la ISO 8583:2003 aún no ha logrado una amplia aceptación.

[0022] Un mensaje de ISO 8583 está compuesto por las siguientes partes:

Un indicador de tipo de mensaje (MTI)

Uno o más mapas de bits, que indican cuales elementos de datos están presentes

Elementos de datos, los campos del mensaje.

[0023] Los dispositivos o sistemas remotos que pueden acceder el sistema de la presente invención incluyen una caja registradora electrónica (ECR) (no se ilustra); Un módulo de Respuesta Interactiva de Voz (IVR) 101, un dispositivo de punto de venta (POS) 109, que puede comunicarse con un campo lector de comunicaciones cercano (NFC) para leer la información desde una tarjeta de crédito o dispositivo móvil, por ejemplo, un dispositivo de cómputo con acceso a Internet (Web) 103; un teléfono celular con una aplicación para banca móvil (MB) 107; y un dispositivo remoto capaz de recibir mensajes SMS (SMS) 105. Los dispositivos remotos 101, 103, 107, y 109, pueden comunicarse con la API (*Application Programming Interface*) 141 a través de Internet o los circuitos de la Red de Punto de Acceso (APN). Algunos de estos son dispositivos remotos "smart" (inteligentes) que pueden ensamblar un mensaje modificado ISO 8583 y enviarlo a la API 141. Para otros dispositivos con capacidades limitadas, un servicio de administración de clientes (CMS) (no se ilustra) puede ser utilizado para ensamblar un mensaje modificado ISO 8583 y enviar el mensaje modificado correspondiente ISO 8583 a la API 141. Por ejemplo, El CMS verifica la información recibida por los dispositivos antes de ensamblar el mensaje modificado ISO 8583. en general, el CMS verifica que un número telefónico celular particular exista, como en una incorporación de la presente invención el número telefónico celular de un usuario es utilizado como el número de cuenta, verifica que la cuenta del usuario esté activa, y verifica que el máximo número de autorizaciones (por ejemplo, el número de transacciones permitido por mes, día, etc.) no haya sido excedido. La información verificada y suministrada por el CMS puede ser utilizada para ensamblar mensajes modificados ISO 8583. El CMS entonces puede enviar el mensaje modificado ISO 8583 al AP 141 o este puede reenviar parámetros de verificación a un dispositivo inteligente para el ensamblar del mensaje modificado ISO 8583.

[0024] Como se mencionó, los dispositivos remotos pueden ser utilizados para el intercambio de mensajes modificados ISO 8583 con el API 141, que reside en un servidor de conmutación. Otros componentes del servidor de conmutación pueden incluir un modulo de conmutación, un módulo ATM, un módulo ACH, y un

módulo para utilizar en interfase con otras redes. Una de las funciones del API 141 es convertir los mensajes modificados ISO 8583 en mensajes estándar ISO 8583. Otra función incluye el paso de aquellos mensajes ISO 8583 a otros módulos que son parte del sistema de la presente invención, por ejemplo el módulo de administración del terminal 137 o el módulo de autorización 139. Cuando el API 141 conduce mensajes con esos módulos, por ejemplo, la transacción financiera se conoce como una transacción de circuito cerrado (closed loop transactions). Cuando el API 141 intercambia mensajes con un módulo de conmutación, el modulo ACH o los otros módulos de red en el servidor de conmutación, los mensajes desde el API 141 dejan la arquitectura de red ilustrada en la Fig. 1, y como tal, las transacciones que involucran tal tipo de mensajes se conocen como transacciones de circuito abierto (open loop transactions), como sería comprendido por una persona de conocimiento común en la técnica.

[0025] El sistema de la presente invención puede incluir módulos de procesamiento "front end" (FEP). En una incorporación de la presente invención, el FEP incluye módulos de adquiriente (es decir, los módulos 137-141 que adquieren instrucciones o comandos desde los dispositivos remotos) y módulos de procesamiento (es decir, módulos 143-151 que ejecutan instrucciones para leer o escribir información en la base de datos 153). El FEP puede ser implementado en un servidor separado del servidor de conmutación. En una incorporación de la presente invención, los módulos de adquisición y procesamiento pueden ser implementados como máquinas virtuales separadas que corren sobre el mismo servidor.

[0026] Los módulos de adquisición FEP pueden incluir un módulo de administración de terminal 137, un módulo de administración 139 y un módulo de transacción 141. El modulo de administración de terminal 137 se utiliza para procesar solicitudes desde los dispositivos POS y ECR. Estas solicitudes pueden incluir la identificación del POS o ECR, información del origen de la cuenta, información de la cuenta de destino, y suma de la transacción y de gastos de transacción.

[0027] En una incorporación, la transacción que solicita desde dispositivos remoto diferentes de un POS o ECR se puede pasar por el API 141 directamente

en el modulo de autorización 139. El modulo de autorización 139 verifica si la cuenta a ser debitada tiene saldo suficiente para completar la transacción, que el PIN ingresado para autenticación del usuario (por ejemplo, PIN1) concuerde con el PIN almacenado en la base de datos 153, y verifique que el número de autorización se cumpla. El PIN es internamente recreado por el modulo de contraseña y criptografía 147, el cual puede ser implementado como una tarjeta de criptografía con base en un hardware. Tras la autorización, el modulo 139 emite un código de autorización. En una incorporación, los dos últimos dígitos del código de autorización pueden ser utilizados como un código de uso temporal/ de una sola vez (es decir, PIN2) para realizar las transacciones por ATM o las transacciones de compras.

[0028] El código de autorización se pasa al modulo de transacción 141, que genera instrucciones para créditos o cuentas escritas, post débito a cuentas, así como honorarios. Por ejemplo, si la transacción solicitada es para una compra, el modulo de transacción 141 instruye al modulo de servicios mercantil 145 a inscribir un crédito en la cuenta del comerciante en la base de datos 153, instruye al módulo de tarjeta débito 143 para inscribir un débito en la cuenta del usuario en la base de datos 153, e instruye la facturación y al módulo de alimentación administrativa 151 para fijar unos honorarios asociados con la transacción. Como las transacciones han sido completadas, el modulo de administración de archivos 149 guarda un registro de las transacciones procesadas (por ejemplo, tiempo de transacción, etc.) 141.

[0029] En otro aspecto de la presente invención, la base de datos 153 es compartida por los módulos FEP y el procesamiento back end (parte que procesa la entrada) del (BEP). En la incorporación ilustrada, los módulos BEP incluyen el módulo de información de clientes 155, el módulo de manejo de flujo de caja 157, el módulo de cuentas de ahorro 159, el módulo de producto financiero 161, y el módulo de inversión 163. Estos módulos BEP están asociados con funciones tradicionales de banca. En una incorporación, éstos pueden ser implementados como módulos utilizados para crear reportes que contengan información básica del cliente (155), información acerca del manejo del flujo de caja de un cliente (157), información relacionada con los ahorros de un cliente (159), información acerca de productos financieros utilizados por un cliente (161), e información acerca de las inversiones de un cliente (163).

[0030] Una de las ventajas de la presente invención es que los usuarios del sistema pueden activar o crear cuentas sin la necesidad de someterse a todas las formalidades impuestas bajo un modelo bancario tradicional. En consecuencia, algunas de las funciones bancarias más tradicionales asociadas con el procesamiento BEP puede que no sean necesarias para un usuario de la presente invención. Por ejemplo, en una incorporación preferida, un usuario puede ir a un almacén o tienda que opera un POS para abrir una cuenta con una NBFi o banco, o para abrir en una NBFi o banco una cuenta débito prepagada que tenga un límite en términos de número de transacciones y límite de efectivo así como los medios para informar acerca del lavado de dinero a las autoridades. El sistema aun permite que estas transacciones tengan lugar en el sitio. La presente invención no inhibe el proceso KYC (Know Your Client – Conozca a su Cliente) si es obligatorio y el BEP permite el procesamiento de transacciones que involucran contacto cara a cara para la creación de cuentas o el proceso simplificado de creación de cuentas de la incorporación preferida de la presente invención. El usuario o cliente nuevo le entregaría dinero en efectivo al comerciante para depositar en una cuenta asociada con el número telefónico del móvil de tal cliente. Utilizando la interfase IVR 101, un cliente de una NBFi o banco que implemente el sistema de la presente invención puede marcar en el sistema para encontrar información de saldos, Transacciones autorizadas, etc. Utilizando la interfase de red, un usuario del sistema, por ejemplo un empleador, puede iniciar sesión en el sistema y autorizar los pagos de nómina mediante la transferencia de fondos de una NBFi o banco, por ejemplo, a la cuenta de un empleado. También, el sistema de la presente invención puede enviar mensajes de texto (por ejemplo SMS) para confirmar que las transacciones han sido completadas. Estas transacciones ejemplificantes serán discutidas en detalle más adelante.

[0031] La Fig. 2 ilustra un tipo de transacción que puede ser ejecutada a través del uso de un POS en el cual un nuevo cliente de la NBFi o banco que utiliza la presente invención puede activar una cuenta en la ubicación de un comerciante. El comerciante es designado como Correponsal Independiente o tienda autorizada por el banco o la NBFi. Un cliente puede hacer un depósito inicial en una ubicación seleccionada, por ejemplo, en cualquiera de las tiendas asociadas o Corresponsales Independientes. En el paso 201 un comerciante podría ingresar en el POS 109, por ejemplo, el número celular asociado con el nuevo cliente. El

cliente podría esperar hasta que el sistema le llame para verificar la identificación del propietario del teléfono celular. El cliente entonces, podría escoger un PIN (paso 203) y este PIN es ingresado en la conexión POS al FEP para aprobar una autorización solicitada por el dispositivo POS, que forma parte del paso de configuración de la cuenta 205, para reiniciar el cumplimiento de la solicitud mediante la introducción de un código temporal suministrado al Comerciante por el sistema, que permite a la transacción seguir adelante con todos los parámetros incluidos habilitados por el intercambio de información entre el titular de la cuenta (vía Telefónica), El comerciante que suministra la facturación y permite el pago electrónico con confidencialidad de la información, y la validación y la decisión por el consumidor para completar el pago, y la notificación de la decisión con el código temporal al operador del POS del Comerciante. El POS entonces obtendrá los parámetros de confirmación y adicionales para verificar la validez y la información acerca del propietario de la cuenta. El sistema de la presente invención sería entonces configurar la cuenta en el paso 205. Tras la recepción del efectivo y tras los métodos de activación de cuenta por la NBFi o el Banco, el comerciante puede introducir el número del titular de la cuenta del teléfono celular en el POS 109 en los pasos 207 y 209 para abonar en la cuenta al recibir el efectivo para "acreditar" la cuenta. Luego de que la cuenta ha sido financiada (fondeada), el cliente recibe un mensaje de texto vía un Sistema de Mensaje Corto (SMS) la confirmación de la transacción en su teléfono celular a través de un mensaje SMS (en la parte superior de la cantidad anterior a debitar de su cuenta por (IVR), por ejemplo (paso 211).

[0032] La Fig. 3 ilustra un método para transferir dinero en efectivo de un titular de cuenta en una NBFi o banco a otra. En el paso 301 el usuario selecciona la opción de transferencia de efectivo en un menú presentado por el MB 109 o Web 107, por ejemplo luego de que el MB 109 o Web 107 reconoce una transferencia o cuenta en particular, el usuario entonces ingresa el número de teléfono celular asociado con el otro titular de cuenta (paso 303) o número de tarjeta débito en la cuenta de destino así como la cantidad a ser transferida y el PIN de autenticación del usuario (es decir, PIN 1). La aplicación instalada en la terminal Web 107 o teléfono celular MB 109 entonces se comunica con el CMS para obtener la verificación de que los números de celular existen (permitido por la señalización de la red y la base de datos en CMS con los números registrados y cuenta asociada), que las cuentas están activas y verifica el número total de permisos para quien

transfiere (paso 305). En el paso 307 la aplicación de teléfono o red construye un mensaje modificado ISO 8583 sobre la información suministrada por el CMS y la envía al API 141.

[0033] En el paso 309 el API 141 convierte el mensaje recibido de un ISO 8583 modificado a un ISO 8583 estándar y el módulo de autorización 139 emite un código de autorización si la cuenta del usuario tiene fondos suficientes, el número de autorizaciones no es excedido, y otra información de los usuarios finales, tal como el PIN, es validada. En el paso 311 el modulo de transacción 141 se comunica con el modulo de servicios del comerciante 145 y el modulo de tarjeta débito 143 y encarga a estos módulos colocar el débito y el crédito en la base de datos 153 con respecto a las cuentas involucradas en la transacción. El modulo de transacción también instruye al modulo 151 para calcular y fijar los honorarios asociados con la transacción, si los hay. En el paso 313 el modulo de autorización informa a la red o aplicación de teléfono que reside en la Web 107 o MB 109 que la transacción ha sido aprobada y también elabora un mensaje que es enviado al usuario a través de la interfase SMS 111. El cedente y el cesionario reciben una confirmación por mensaje de texto (por ejemplo, SMS) de la transferencia.

[0034] La Fig. 4 ilustra un método para recuperar efectivo desde una NBFÍ o ATM autorizado de un banco de acuerdo con una incorporación de la presente invención. Esta transacción es preparada por el Cliente (usuario final) por anticipado por una suma específica utilizando la funcionalidad IVR. En el paso 401 el sistema recibe una solicitud para retiro de efectivo en un ATM, por ejemplo un ATM franquiciado a la marca o permite a una Red de ATM con la no solicitud de tarjeta del presente sistema. Si la solicitud es efectuada en el ATM, la solicitud puede ser activada por una tecla de función o una tecla pulsada por el usuario para indicar que el usuario busca retirar efectivo sin utilizar una tarjeta de ATM. La solicitud debe ser acompañada por el número celular del usuario. Antes de enviar la solicitud al API 141, el ATM se comunica con la Base de Datos CMS para determinar si la cuenta del usuario es válida, etc. En el paso 403, el ATM envía la solicitud al modulo de autorización 139 en el FEP a través de una interfase ATM (Aplicación ATM HUB para cambio de la transacción a FEP utilizando el estándar de mensaje ISO8583) y el FEP determina si la solicitud es aceptada o declinada (de acuerdo con los parámetros establecidos por las solicitudes del usuario cuando preparó la solicitud de retiro del ATM a través del IVR), basado en si la

cuenta asociada con el número telefónico celular está activa como una primera verificación para aprobar/declinar antes de proceder. Si la solicitud no es aceptada, el sistema genera una respuesta con un mensaje negando la solicitud de retiro. Por ejemplo, el usuario puede recibir un mensaje de texto (o el ATM puede mostrar tal mensaje) que informa que la solicitud ha sido denegada. En el paso 407, si la solicitud es aceptada, el usuario puede recibir un mensaje de texto con un código de autorización temporal para ingresar (PIN2). En una incorporación, este código temporal puede ser los dos últimos dígitos de un código de autorización generado por el módulo de autorización 139 en respuesta a la solicitud original.

[0035] En el paso 409, el usuario puede ingresar el código temporal junto con un PIN de usuario (PIN1) y la suma a ser retirada. En el paso 411, el ATM requiere a la NBTI licenciada o al banco solicitar una autorización ISO8583 para suministrar efectivo. Mientras esta solicitud está basada en ISO8583, las comunicaciones entre el ATM y el FEP están basadas en el ISO8583 modificado de la presente invención. En el paso 413, el emisor (banco licenciado o NBTI) autoriza el retiro de efectivo basado en PIN2 así como en parámetros adicionales. En el paso 415, el ATM recibe y procesa información para autorizar la transacción, este dispensa el efectivo, y este mensaje SMS se envía al usuario confirmación de la transacción.

[0036] La Fig. 5 ilustra a un alto nivel un método para la recuperación de efectivo en una ubicación de comerciante, a manera de ejemplo. Un método más específico puede ser implementado mediante el uso de un método similar al método descrito con respecto a la Fig.4 excepto que el usuario de la interfase podría ser un POS en lugar de un ATM. En referencia a la Fig.5, en el paso 501 un usuario solicita al comerciante efectivo. En el paso 503 el comerciante ingresa el final - en el POS. En el paso 505 el comerciante ingresa el número de teléfono celular del usuario, la suma de los retiros, y el PIN1 en la aplicación POS. En el paso 507 el comerciante ingresa una solicitud para autorización con el PIN2 (dos últimos dígitos de la sesión ID a ser incluidos en una transacción POS para completar la solicitud modificada ISO8583 o completar la autorización) recibe texto con la confirmación de que se puede ofrecer efectivo al usuario, asumiendo que el usuario tiene fondos. En el paso 509 el comerciante ofrece efectivo y las cuentas

del comerciante se acreditan en el procesador back-end que da soporte a los servicios del comerciante.

[0037] La Fig.6 ilustra un método para comprar bienes en el local del comerciante. Luego de que el cajero haya obtenido el monto total adeudado para la venta de bienes, el usuario suministra un número de teléfono celular asociado con la NBFi o cuenta bancaria al cajero (paso 601). En el paso 603 el cajero ingresa, a través de un ECR (o un dispositivo POS), el número de teléfono celular y la suma debida en el sistema. En el paso 605, el ECR construye un mensaje modificado ISO8583 solicitando autorización y enviándola al Módulo de Administración de Terminal 137 en el FEP. En una incorporación, el mensaje modificado ISO 8583 es construido luego de una verificación de que ciertos datos de usuario son recibidos desde CMS, como se describió anteriormente. En el paso 607 el FEP encuentra los parámetros de parte variable en el mensaje, activa un mensaje desde el API 141 utilizando una rutina POS/ECR cargada en el FEP, e inicia la rutina de interfase de voz (AGI, que representa Asterisk Graphics Interface). El sistema de voz de AGI hace una llamada al usuario y obtiene autorización del usuario una vez ingresa su número PIN asociado con la cuenta (paso 609). En el paso 611 el AGI se comunica con el API en el FEP y suministra un código temporal para usuario. En una incorporación, el código temporal puede ser los dos últimos dígitos de un código de autorización emitido por el módulo de autorización 139. En el paso 613, las claves de comerciante en el código temporal suministrado por el usuario para forzar la ECR/POS a reestructurar el mensaje modificado ISO 8583, envía el mensaje al API 137, y cierra la transacción.

[0038] La Fig.7 ilustra un método que puede ser utilizado por un empleador para hacer los pagos de nómina a sus empleados. En el paso 701 el empleador se registra en su cuenta a través de una interfase de red y luego autoriza el desembolso de la nómina. Este pago puede ser una transferencia de NBFi o cuenta de banco a una o más NBFi o cuentas de banco. En el paso 703 una aplicación de red solicita que la Base de Datos CMS verifique que la cuenta del empleador está activa, por ejemplo, y que el número de autorizaciones asociadas con la cuenta del empleador no han sido excedidas. Tras la verificación, en el paso 705 la aplicación de red construye un mensaje modificado ISO8583 y comunica el mensaje a la API 141. En el paso 707, el API 141 convierte el mensaje en un mensaje estándar ISO8583, y el modulo de autorización 139 emite

un código de autorización si la cuenta del empleador tiene saldo suficiente, el número de autorizaciones no es excedido, y otra información del empleador es válida. En el paso 709 el modulo de transacción 141 instruye a los módulos de procesamiento correspondientes en el FEP para escribir los créditos y débitos a las cuentas del empleador y empleado, junto con los costos asociados. En el paso 711 el modulo de autorización informa a la aplicación de red que las transacciones han sido aprobadas y elabora mensajes SMS que son enviados a los empleados y el empleador para confirmar los desembolsos.

[0039] La Fig. 8 ilustra un método para hacer pagos a un beneficiario (por ejemplo, una empresa de servicios públicos). En el paso 801 un usuario accesa a una aplicación de teléfono celular o marca en un sistema IVR para banca móvil. En el paso 803 el usuario accesa a una lista de beneficiarios mostrada en el teléfono celular o comunicada al usuario a través de la interfase IVR. El usuario selecciona al beneficiario e ingresa la información de cuenta del beneficiario, la suma a pagar, y un PIN.

[0040] En el paso 805 la Base de Datos CMS verifica que la cuenta del usuario esté activa y válida y verifica que el número de autorizaciones no haya sido excedido. Si el usuario está accedendo el sistema a través de la interfase MB 107, la aplicación del teléfono celular envía la solicitud para verificación al CMS y no elabora un mensaje modificado ISO 8583 hasta que el CMS verifica la cuenta del usuario. Si el usuario está accedendo el sistema a través de la interfase IVR 101, el CMS recibe la solicitud para verificación pero no necesita responder a la interfase IVR 101.

[0041] En el paso 807, la aplicación del teléfono celular elabora el mensaje modificado ISO 8583 para solicitar la transacción de pago al sistema cuando el usuario solicita tal transacción a través del MB 107. Alternativamente, el CMS con un guión de programa se adecuó para la elaboración del mensaje modificado ISO 8583 cuando el usuario solicita la transacción a través del IVR 101. Luego, o el MB 107 o el CMS envían el mensaje modificado ISO 8583 al API 141.

[0042] En el paso 809 el API 141 convierte el mensaje modificado ISO 8583 en un mensaje estándar ISO 8583 y envía el mensaje convertido, junto con parámetros en la parte variable del mensaje modificado ISO 8583, al módulo de

autorización 139. El modulo de autorización 139 entonces emite un código de autorización si la cuenta del usuario tiene saldo suficiente, el número de autorizaciones no ha sido excedido, y otra información de usuario es válida (por ejemplo, el PIN). En el paso 811 el modulo de transacción 141 instruye a los correspondientes módulos de procesamiento en el FEP para inscribir un crédito y débito a las cuentas correspondientes, junto con los costos asociados. En el paso 813, el modulo de autorización 139 elabora un mensaje SMS para informar al usuario que la factura ha sido pagada. Alternativamente, el modulo de autorización 139 elabora un mensaje IVR para informar al usuario a través de la interfase IVR 101 que la factura ha sido pagada.

[0043] Como ha sido mencionado, estas transacciones tienen lugar sin que el usuario haga uso de internet como el o ella tendrían que ver con la banca móvil convencional. La interfase entre el usuario y el sistema está basada en una variante del ISO 8583 como se explicó anteriormente. El formateo del mensaje modificado ISO 8583 será explicado a continuación. Los mensajes intercambiados entre el servidor de interfaz con los usuarios y el FEP también están basados en el estándar ISO8583.

[0044] Todas las transacciones anteriores pueden ser medidas en una Base de Datos CMS Primaria y otros módulos para elaborar el mensaje utilizando una secuencia de comandos específicos relacionados con todas las interfases que usan una librería escrita XML para el uso particular, de acuerdo con una incorporación de la presente invención. Tal Base de Datos sirve para controlar la actividad del usuario (incluyendo fraccionamiento de transacciones para esconder lavado) y límites de exposición o uso abusivo por los clientes y puede ser considerada un mecanismo de prevención de fraude. Tal Base de Datos está conectada a componentes de voz, mensajería, registro en la red y registro en la banca móvil. Se mide la actividad global de las cuentas de usuario independientemente de la interfase seleccionada por el usuario. Por ejemplo, en el sistema de procesamiento de voz este permite el enrutamiento cuando un número de teléfono celular asociado a una cuenta existe y bloquea el uso cuando la cuenta está marcada por cualquier razón o esta ha sido desactivada o no existe. Tal flujo de llamadas e intercambio de información puede ser controlado por una secuencia de comandos que manejan la capacidad de conmutación de voz y todas las otras interfases que intercambian la información a través de mensajes via XML.

Formato ISO 8583 Modificado

[0045] Los servicios de la industria financiera incluyen el intercambio de mensajes electrónicos relacionados con transacciones financieras. Un esfuerzo internacional fue llevado a cabo por la Organización Internacional de Estándares (ISO – por sus siglas en inglés) con una meta principal de defender una estructura única de mensaje para ser utilizada por todas las instituciones financieras alrededor del mundo. La ISO 8583 es el nombre del estándar internacional para transacciones financieras con mensajes originados en una tarjeta. Este define específicamente una estructura única de datos para el intercambio de mensajes entre redes financieras heterogeneas. Específicamente, el estándar determina una interfase común por la cual mensajes originados por una tarjeta de transacción financiera pueden ser intercambiados. Este especifica estructura, formato y contenido, elementos y valores de datos. Una ventaja de la presente invención es que permite a los usuarios llevar a cabo transacciones financieras, por ejemplo, compras sin la necesidad de una tarjeta débito o crédito mediante la conversión de los mensajes ISO 8583 modificados para que la red financiera “vea” la transacción sin tarjeta como una transacción de crédito o débito en total cumplimiento de parámetros obligatorios.

[0046] Las estructuras de mensajes ISO8583 tienen una serie de campos donde los datos transaccionales relacionados son almacenados. Estos campos son referidos como Bitmaps. La combinación de bitmaps distintos es lo que hace a las transacciones financieras que puedan ser procesadas por una institución financiera.

[0047] El estándar ISO8583 es únicamente el boceto principal a seguir por una entidad financiera con el fin de implementar las unidades transaccionales. La especificación de la aplicación puede permanecer en un nivel privado. Los diseñadores de la aplicación tienen completa libertad de diseño, dentro de la restricción general de la ISO 8583, para que tales mensajes sean convertibles al formato de interfase ISO 8583 para que el intercambio internacional pueda llevarse a cabo. La idea es que los desarrolladores de la aplicación financiera sean libres para implementar lo que consideren necesario si y únicamente si sus interfases de mensajes pueden ser trasladadas a especificaciones ISO8583 con el fin de promover el intercambio internacional.

[0048] La presente invención aprovecha la flexibilidad de la ISO 8583 mediante la implementación de una interfase común de mensajes enfocada en los datos para ser intercambiados en lugar de la complejidad de los esquemas en el mensaje de designación y declaración de esquemas de bitmap ISO 8583 en el mensaje. Esta característica se conoce aquí como la Parte Fija, Marcos de Mensajería de la Parte Variable, interfase. Uno de los beneficios de esta interfase ISO 8583 modificada es la facilidad de comunicación transaccional entre aplicaciones financieras de terceros y los procesadores back end convencionales que requieren conversión al estándar ISO8583.

Estructura de Datos de Parte Fija Parte Variable

[0049] En una incorporación de la presente invención, el intercambio de datos entre los módulos front-end y las aplicaciones de usuario final utilizados para interfase con la NBFi o el banco están basados en el uso de las Estructuras de Datos de Parte Fija Parte Variable. De acuerdo con esto, los datos para transacciones son puestos juntos en marcos específicos donde cada dato tiene una posición específica en el marco.

[0050] Los Marcos de Parte Fija / Parte Variable están basados en las premisas de la ISO 8583. La primera sección de un marco de comunicación a partir de esta implementación se denomina Parte Fija en el presente y contiene toda la información compartida que pertenece a todas las transacciones en el sistema, por ejemplo, el momento cuando las transacciones fueron ejecutadas, el código de transacción, el código de respuesta, y otros. La segunda sección del marco se denomina en el presente como la Parte Variable y permite enviar datos específicos dependiendo de la transacción que será ejecutada. Por ejemplo, si la operación que será ejecutada es Saldo de la Cuenta, entonces en la Parte Variable del mensaje ISO 8585 modificado, será enviado un mensaje con información básica del usuario. La sección de Parte Variable también permite establecer comunicación con terminales bancarias no tradicionales tales como teléfonos móviles y dispositivos POS. En una incorporación, el marco de Parte Fija, incluye 250 caracteres mientras que la Parte Variable es variable en su longitud.

[0051] La estructura de la parte Fija puede definirse como sigue:

DESCRIPCION	I/O	TIPO	LONGIT.	Decimal es	Des de	Hasta	Valores/Restricciones
Código de Aplicación	O	A	2		1	2	Valor Fijo = CS : Indica a FEP una transacción desde NBFU OPERADOR BANCARIO LICENCIADO
Código de Transacción	O	A	6		3	8	Indicador Alfanumérico que define códigos a ser interpretados por el Núcleo y corresponden a una transacción específica a ejecutar Este campo tiene la siguiente estructura: XXYYZZ XX código para indicar el tipo de transacción. YY Código para indicar el tipo de cuenta que origina la transacción ZZ código para indicar el tipo de cuenta de destino.

DESCRIPCION	I/O	TIPO	LONGIT.	Decimal es	Des de	Hasta	Valores/Restricciones
CódigoCajero	O	A	9		9	17	000000000 Este campo puede ser llenado con nueve ceros.
Código de Oficina	O	A	3		18	20	000 Este campo puede ser llenado con tres ceros
Fecha de la Transacción	O	N	8	0	21	28	YYYYMMDD Ejemplo: 20090122 Corresponde a Enero 22 de 2009.
Hora de la Transacción	O	N	6	0	29	34	HHMMSS Ejemplo: 142510 Corresponde a 14 horas 25 minutos 10 segundos
Fecha Efectiva de la transacción	O	N	8	0	35	42	YYYYMMDD Este campo tiene que tomar el mismo valor del campo Fecha de Transacción en una solicitud.
CódigoCanal	O	A	3		43	45	Valor Fijo= IVR
SwitchCode	O	N	4	0	46	49	Código Numérico que identifica las acciones a ser seguidas en el Núcleo Transaccional

DESCRIPCION	I/O	TIPO	LONGIT.	Decimal es	Des de	Hasta	Valores/Restricciones
Dispositivo	O	A	2		50	51	Valor Fijo= 02(Valor cambiado)
Número Correlativo	O	N	12	0	52	63	Representa un contador para todas las transacciones, el código es puesto en cero todos los días. Puede ser manejado por la aplicación IVR.
Número de Autorización	I	N	6	0	64	69	Puede ser llenado con 000000 para el Mensaje del Módulo API que invoca. El núcleo puede responder con un valor numérico de 6 posiciones
Tipo de Transacción	O	A	1		70	70	1 = Transacción Normal 2 = Transacción Forzada 3 = Reversión de Transacción
Código de Respuesta	I	A	5		71	75	Puede ser llenado con 00099 para el Mensaje del Módulo API que invoca. El núcleo puede responder con un valor numérico de 5 posiciones

DESCRIPCION	I/O	TIPO	LONGIT.	Decimal es	Des de	Hasta	Valores/Restricciones
Descripción del Código de l Respuesta	I	A	75		76	150	Puede ser llenado con 75 blancos para el Mensaje del Módulo API que invoca. El núcleo puede responder con un valor alfanumérico de 75 posiciones relleno con blancos si es necesario.
Relleno	O	A	99		151	250	Puede ser llenado con 99 blancos

[0052] Como se señaló al principio, cada transacción implementa su propia parte variable dependiendo de su naturaleza y funcionalidad.

[0053] La presente invención permite las siguientes transacciones vía interfase de la Parte Fija, la Parte Variable (es decir, la interfase ISO 8583 modificada):

Código de Procesa miento	Descripción	Tipo	Canal de Adquisic ión	Switc h
330000	Consulta de Saldo (Número de Cuenta)	No Monetaria	IVR	2021
330000	Consulta de Saldo (Número de Cuenta)	No Monetaria	WEB	2023
330000	Consulta de Saldo (Número de Cuenta)	No Monetaria	MB	2026
311000	Consulta de Saldo (Número de	No Monetaria	WEB	2023

Código de Proceso	Descripción	Tipo	Canal de Adquisición	Switch
	ID)			
311000	Consulta de Saldo (Número de ID)	No Monetaria	MB	2026
330000	Consulta de Saldo (Número de Cuenta)	No Monetaria	SMS	2028
321000	Consulta de Último Movimiento Monetario	No Monetaria	IVR	2021
321000	Consulta de Último Movimiento Monetario	No Monetaria	SMS	2028
321000	Consulta de Último Movimiento Monetario	No Monetaria	WEB	2023
330000	Consulta de Saldo (Número de Cuenta)	No Monetaria	WEB Corporat	2024
330000	Consulta de Saldo (Número de ID)	No Monetaria	WEB Corporat	2024
321000	Consulta de Último Movimiento Monetario	No Monetaria	MB	2026
321000	Consulta de Último Movimiento Monetario	No Monetaria	WEB Corporat	2024
401030	Transferencias a Terceras Partes	Monetaria	IVR	2021
401030	Transferencias a Terceras Partes	Monetaria	WEB	2023
401030	Transferencias a Terceras Partes	Monetaria	MB	2026
500002	Inicio de Sesión	No Monetaria	WEB Corporat	2024
500002	Inicio de Sesión	No Monetaria	WEB	2023

Código de Proceso	miento Descripción	Tipo	Canal de Adquisición	Switch
500002	Inicio de Sesión	No Monetaria	MB	2026
500003	Cambio de PIN de Acceso	No Monetaria	WEB Corporat	2024
500003	Cambio de PIN de Acceso	No Monetaria	WEB	2023
500003	Cambio de PIN de Acceso	No Monetaria	MB	2026
500006	Recuperación de PIN de Acceso (Restablecimiento de Indicador)	No Monetaria	WEB	2023
500006	Recuperación de PIN de Acceso (Restablecimiento de Indicador)	No Monetaria	WEB Corporat	2024
500001	Recuperación de PIN de Acceso (ajuste de PIN)	No Monetaria	WEB Corporat	2024
500001	Recuperación de PIN de Acceso (ajuste de PIN)	No Monetaria	WEB	2023
500007	Recuperación de PIN de Acceso (Restablecimiento de Indicador)	No Monetaria	WEB	2023
500007	Recuperación de PIN de Acceso (Restablecimiento de Indicador)	No Monetaria	Corporat e WEB	2024
330000	Consulta de Saldo # Cuenta/Teléfono Celular	No Monetaria	POS	2014
340000	Consulta de Saldo # Cuenta/Teléfono Celular	No Monetaria	POS	2014
001000	Compra de Bienes y Servicios (Tarjeta)	Monetaria	POS	2014
061001	Compra de Bienes y Servicios (Teléfono Celular)	Monetaria	POS	2014

Código de Proceso	miento Descripción	Tipo	Canal de Adquisición	Switch
261001	Compra de Bienes y Servicios (Teléfono Celular) Inválida	Monetaria	POS	2014
061002	Verificación IVR PIN Compra de Bienes y Servicios	Monetaria	POS	2014
261002	Verificación IVR PIN Compra de Bienes y Servicios Inválida	Monetaria	POS	2014
201000	Compra de Bienes y Servicios Inválida	Monetaria	POS	2014
021000	Recarga de Cuenta	Monetaria	POS	2014
221000	Recarga de Cuenta Inválida	Monetaria	POS	2014
031000	Redención	Monetaria	POS	2014
231000	Redención Nula	Monetaria	POS	2014

Aplicación de Software de Banco Celular

Funcionalidad

[0054] El Banco Celular o Aplicación de Banca Móvil de la presente invención permite a la NBFi o a los clientes del banco completar transacciones bancarias comunes (por ejemplo, consultas de saldo, transferencias) utilizando un teléfono móvil. Esto permite a la NBFi o a los clientes del banco administrar sus cuentas bancarias desde cualquier ubicación donde haya acceso a señal de teléfono móvil o conexión a Internet.

[0055] La aplicación de Banco Celular de la presente invención puede estar basada en un Midlet J2ME. El Midlet J2ME permite a una NBFi o a los clientes del Banco y al NBFi o al banco comunicarse en una red de datos utilizando una red de datos de operador con conexión telefónica inalámbrica. La aplicación de Banco Celular de la presente invención se comunica con una puerta de entrada de banca móvil para autorizar a un cliente a utilizar la aplicación. La puerta de entrada de banca móvil valida una sesión de usuario y procesa mensajes de entrada y salida

para y desde la Aplicación de Banco Celular. También es responsable por comunicarse con el FEP para enviar mensajes ISO 8583 modificados de las transacciones generadas.

Arquitectura de la Aplicación

[0056] La Aplicación de Banco Celular de la presente invención puede suministrar una serie de aplicaciones integradas configuradas para correr en un esquema de cliente-servidor. En una incorporación, la aplicación de cliente reside en un teléfono móvil de un usuario y adquiere y administra datos que pueden ser necesarios para una transacción en la red del Sistema de Pagos Electrónicos NBFÍ (EPS) de transacciones de bajo valor o un FEP Bancario utilizando la conversión ISO 8583 cuando se ensamblan las transacciones o comunicaciones a la cuenta. La aplicación del cliente utiliza las capacidades de comunicación suministradas por el teléfono móvil para iniciar una conexión de datos con servidores intermediarios que actúan como middleware entre el cliente y la NBFÍ o el banco.

[0057] La arquitectura de conectividad está basada en las características definitorias de los actuales teléfonos móviles, es decir, la capacidad de acceder a la Internet a través de la red celular y transferir datos vía el protocolo HTTP. La arquitectura de comunicación revelada aprovecha la accesibilidad de Internet, transferencia de datos vía el protocolo HTTP, y el creciente poder de cómputo/procesamiento de los teléfonos móviles, para reducir la cantidad de datos intercambiados sobre las plataformas tecnológicas en las que se basa la Aplicación de Banco Celular.

[0058] La Aplicación de Banco Celular de la presente invención puede residir en el teléfono móvil del cliente. La aplicación puede adquirir los datos necesarios para iniciar una transacción desde la red de transacciones de bajo valor. Esos datos pueden traducirse en y enviarse como mensajes cifrados convertidos en código XML. El código XML puede incluir los datos para iniciación de una transacción y pueden ser entregados por middleware al servidor a través de HTTP POST. El middleware traduce los datos reenviados al formato de intercambio de información apropiado utilizando el ISO8583 modificado de la presente invención.

[0059] El código XML utilizado para iniciar cualquier transacción solicitada utiliza una o más etiquetas que pueden ser definidas en términos de los parámetros necesarios a ser incluidos para cada transacción basados en el estándar ISO8583 modificado utilizado en conexión con la red financiera de transacciones de bajo valor. Adicionalmente, para cumplir con los requisitos básicos de seguridad, un programa de criptografía puede ser utilizado para asegurar la información sensible relacionada con las operaciones del sistema financiero de la presente invención. El programa de criptografía puede suministrar protección ligera y robusta sobre la base de encriptación de información sensible como se especifica, por ejemplo, en W3C: XML Encriptación Sintaxis y Procesamiento.

[0060] Es importante tener en cuenta que, preferiblemente, solo cierta información es encriptada por razón de los altos requerimientos computacionales/de procesamiento de encriptación y desenscriptamiento de grandes cantidades de datos en un tiempo razonable. Tal encriptación y conversión de mensajes opera en una clave temporal hecha como un polinomio de división variable generado por la sesión FEP, que hace a cada transacción única y diferente de la siguiente. En consecuencia, es preferible generalmente encriptar únicamente datos sensibles como PINs, números de cuenta, etc. Pero en este caso tal encriptación genera menos datos y suministra una resolución única en cada extremo. Esto mejora el desempeño del sistema mientras que añade un valor de seguridad adicional. El servidor de middleware puede ser utilizado para implementar el API 141, por ejemplo. El servidor de middleware también puede tener acceso a una base de datos de sesiones y escribe información en tal base de datos para mantener un seguimiento a las sesiones de comunicación entre los usuarios y el servidor de núcleo. El servidor de middleware también tiene acceso a la base de datos que puede contener información para ayudar a la verificación o validación de cuentas de usuario, por ejemplo. El servidor middleware puede conectar con una base de datos de seguridad que puede contener información que puede ser utilizada para validar los PINs.

Referencias de Flujo de Transacción

[0061] Una característica de la Aplicación de Banco Celular de la presente invención es que esta permite a un cliente iniciar una transacción de compra en un punto de venta suministrando al vendedor únicamente el número de teléfono del cliente y un PIN, por ejemplo.

[0062] Tomando en cuenta las variables que entran en juego en este proceso, la transacción es clasificada por el dispositivo del punto de venta como "Tarjeta No Presente." Esta designación hace una transacción de especial cuidado debido a la potencial exposición al fraude por suplantar al usuario real, y en lo que concierne a los negocios, las transacciones clasificadas como "Tarjeta No Presente" enseguida son verificadas con el cliente. El proceso de verificación puede requerir que el cliente sea contactado por teléfono, en donde se le solicita al cliente que confirme o rechace la transacción, mediante el suministro de un código PIN requerido para las transacciones monetarias.

[0063] Como cada transacción es atómica, esta transacción, que en adelante se define como una transacción en el punto de venta "Referencia", puede dividirse en dos pasos independientes de acuerdo con la presente invención. De acuerdo con una incorporación de la presente invención, en el primer paso, una transacción en el punto de venta es pre-autorizada y se mantiene en el conmutador como pendiente de verificación. En el segundo paso, la transacción en el punto de venta es la auto-verificación del cliente. Así el segundo paso es utilizado para verificar el primer paso. Una vez ejecutados ambos pasos, la transacción "Referencia" en el punto de venta es completada.

[0064] Una forma modificada de la transacción "Referencia" es la transacción "Espera Pasiva". La transacción "Espera Pasiva" también es ejecutada utilizando la red de transacciones de bajo valor de la NBFi o el banco. De acuerdo con una incorporación de la presente invención, la transacción "Espera Pasiva" es similar a la transacción "Referencia" en todos los aspectos excepto que el vendedor en el punto de venta solo se hace consciente de la existencia de la transacción al momento de la transacción.

[0065] La FIG. 9 ilustra un proceso que involucra varias transacciones individuales, en su totalidad, apropiadamente sincronizadas, que son referenciadas como "Referencias."

[0066] La Fig. 9 ilustra tres dispositivos o módulos involucrados en el procesamiento de transacciones que involucran referencias, el POS 1401, el módulo de administración de terminal 1403, y una interfase IVR 1405, la cual puede residir en el módulo de autorización 139 (Fig. 1). Para simplicidad, la Fig. no muestra el proceso de conversión de los mensajes desde el estándar ISO 8583 modificado al estándar ISO 8583.

[0067] En una incorporación el flujo de transacción es como se presenta a continuación:

[0068] 1. Un cliente inicia una transacción de compra utilizando un número de teléfono móvil (no necesita una tarjeta plástica débito o crédito) suministrando todos los datos requeridos para la transacción, incluyendo, por ejemplo, el número de teléfono móvil del cliente 1407. El POS genera un mensaje con la información ID Comerciante internamente programada y una serie de caracteres estándar que incluyen los parámetros de transacción tales como fecha, hora, suma y los auxiliares de los códigos de encriptación de seguridad contruidos para Cumplimiento de PCI para otro tipo de transacciones. El mensaje también incluye un código específico que es reconocido por el FEP como una transacción "Referencia". Tal código es parte de la ID de la transacción y se pasa a lo largo del proceso de autorización. El mensaje es enviado al FEP (1451), por ejemplo, al módulo de administración de terminal (1403). El modulo de administración de terminal verifica la suma de la transacción (1409) e identifica la transacción como Transacción Referencia (1411). Al identificar la transacción como una Referencia, el sistema sabe que la realización de la transacción global depende de la verificación de PIN sobre la IVR (1405). Después de la terminación del proceso se presenta un código temporal. Tal código es utilizado para completar el conjunto de todos los parámetros necesarios en la transacción en el POS descrito en el siguiente párrafo.

[0069] 2. El teléfono móvil recibe entonces una solicitud para confirmar la transacción a través del sistema IVR, que solicita al usuario confirmar la transacción con el código de seguridad (PIN1 desde la activación de la cuenta). Una vez recibido y verificado el PIN1 (1413), el IVR comunicará un código de seguridad de un solo uso para que el usuario lo suministre al comerciante. Para

generar un código de seguridad de un solo uso, el administrador del terminal recibe la información del PIN (1419) verifica desde la IVR verifica la vida de la referencia 1421, verifica la información del PIN 1423, y pre-autoriza la transacción 1425. Una vez pre-autorizada se genera un código de pre-autorización y parte de este código puede ser utilizado como el código de seguridad de un solo uso (PIN2).

[0070] 3. Se le envía al vendedor en el punto de venta un mensaje 1453 referenciando la transacción pendiente 1415 junto con una señal de espera 1417, que puede ser mostrada en un monitor o pantalla en el POS. Este mensaje es enviado por el FEP como respuesta a la solicitud de transacción Referencia. La señal de espera puede incluir un mensaje amistoso tal como "Procesando Por favor espere." Al momento en el que la señal de espera es recibida por el vendedor en el punto de venta, los datos necesarios para iniciar el segundo paso de la transacción 1455 han sido enviados por confirmación por el FEP. Este segundo paso puede iniciarse si existe uno de estos dos eventos:

- El cliente ya ha comprobado exitosamente el PIN1 sobre el IVR, para que el cliente pueda aconsejar al vendedor en el punto de venta presionar una tecla o una tecla programada en el monitor que indique "Espera Pasiva," por ejemplo. Presionando la tecla programada "Espera Pasiva" puede ser el desencadenante para el vendedor en el punto de venta para comunicar la respuesta de los datos de verificación de la transacción 1455 recibida como resultado de la primera solicitud de transacción "Referencia".
- El tiempo de espera predeterminado para "espera pasiva" ha caducado, por lo que el punto de venta se convierte en desbloqueado mediante el envío de 1455 los datos de respuesta recibidos de la primera solicitud de transacción "Referencia" para determinar si la transacción puede ser verificada.

4. En ese momento la verificación del PIN ha sido comunicada por el usuario/cliente a través del teléfono móvil, independientemente de que el evento ocurra en el paso anterior tres. Se le pedirá al administrador del terminal verificar si la transacción fue validada por el comerciante con el PIN2 1427 (En una incorporación el IVR suministra PIN2 al cliente y el cliente en retorno suministra PIN2 al comerciante). Este paso involucra las siguientes alternativas:

- El FEP verifica que el comerciante ha suministrado el PIN2 correcto y la transacción es aprobada finalmente. El FEP entonces comunica al vendedor 1431 en el punto de venta que la transacción se aprobó y puede imprimirse un recibo

1433.

- El FEP rechaza la transacción porque el comerciante no suministró un PIN2 correcto. El FEP entonces se comunica con el vendedor 1431 en el punto de venta donde la transacción ha sido rechazada y un recibo de rechazo apropiado puede ser impreso 1433.

La anterior descripción de las posibles implementaciones consistentes con la presente invención no representan una lista completa de todas las implementaciones o todas las variaciones de implementaciones descritas. La descripción de únicamente algunas de las implementaciones no debe interpretarse como un intento de excluir otras implementaciones. Por ejemplo, los expertos entenderán como implementar la invención de muchas otras formas, utilizando equivalentes y alternativas que no se aparten del ámbito de la invención. Además, a menos que se indique lo contrario en la descripción precedente, ninguno de los componentes descritos en las implementaciones son esenciales para la invención. Por lo tanto, se pretende que la especificación y los ejemplos sean considerados como ejemplificantes solamente, con un verdadero alcance y espíritu de la invención indicada por las siguientes reivindicaciones.

REIVINDICACIONES

Lo que se Reivindica es:

1. Un sistema para procesamiento electrónico de transacciones financieras que comprende: Al menos un dispositivo remoto para el montaje de los mensajes de datos en un primer formato, los mensajes de datos incluyen solicitudes de autorización para realizar transacciones financieras sin tarjeta basadas en el uso de un número de teléfono móvil como una referencia a una cuenta de usuario (o una combinación de número de acceso, la selección al responder a múltiples cuentas o productos financieros vinculados al número Telefónico); una aplicación de interfase de programa que reside en un servidor para recibir y convertir dichos mensajes de datos en un segundo formato; un modulo adquiriente que adquiere y decodifica instrucciones en los mensajes de datos que tienen un segundo formato; y un modulo de procesamiento para ejecutar instrucciones adquiridas por el modulo adquiriente para leer o escribir información en una base de datos back end; en donde el modulo adquiriente además se comunica con el dispositivo remoto para informar al dispositivo remoto si la transacción financiera solicitada ha sido aprobada.
2. El sistema de la reivindicación 1, en donde el módulo adquiriente incluye un módulo de autorización o un módulo de transacción.
3. El sistema de la reivindicación 2, donde el dispositivo remoto incluye un dispositivo de punto de venta o una caja registradora electrónica y el módulo adquiriente incluye un módulo de administración de terminal para el procesamiento de solicitudes desde el dispositivo de punto de venta o la caja registradora electrónica.
4. El sistema de la reivindicación 2, en donde el módulo de autorización verifica: Si una cuenta a ser debitada tiene el suficiente saldo para completar la transacción solicitada; Si un PIN ingresado en un dispositivo remoto coincide

con un PIN almacenado en la base de datos backend; o Si un número de autorizaciones es cumplido.

5. El sistema de la reivindicación 2, en donde el modulo de autorización emite un código temporal a ser utilizado como un token de seguridad en la realización de transacciones financieras.

6. El sistema de la reivindicación 5, en donde el código temporal comprende los dos últimos dígitos de una ID de sesión.

7. El sistema de la reivindicación 1, en donde el primer formato es ISO 8583 modificado para incluir una parte fija y una parte variable.

8. Un método para procesamiento de transacciones electrónicas que comprende la creación de una cuenta de usuario, el método comprende: Recibir un número de teléfono celular asociado con un nuevo usuario; Activar una llamada a través de un sistema de respuesta de voz interactivo para verificar la identificación del usuario y la propiedad del teléfono celular por tal usuario; Recibir a través de un punto de venta un número de identificación personal del nuevo usuario; Configuración de una nueva cuenta de usuario; Recibir, a través del punto de venta, una suma de depósito y el número de teléfono celular del usuario; Generar un código temporal y comunicar dicho código al punto de venta; Recibir el código temporal a través del punto de venta; y Financiación de la cuenta de usuario.

9. El método de la reivindicación 8, además comprende la transmisión de un mensaje de texto al usuario para confirmar que la cuenta ha sido configurada y financiada.

10. Un método para transferir efectivo desde una primera cuenta de usuario a una segunda cuenta de usuario, el método comprende: Recibir el número celular asociado con la cuenta del segundo usuario, la suma de la transferencia y el número de identificación personal asociado con la cuenta del primer usuario;

Validar el número de teléfono celular recibido y la cuenta del segundo usuario en un CMS; Validar el número de autorizaciones de cuenta de primer usuario en el CMS; Recibir en una interfase de aplicación de programa una solicitud para transferencia en un primer formato; Convertir la solicitud a un segundo formato y enviar el mensaje convertido a un módulo de autorización; Crear en el modulo de autorización un código temporal si el primer usuario tiene los fondos suficientes; y Acreditar en la cuenta del segundo usuario.

11. El método de la reivindicación 10, además comprende: transmitir un mensaje de texto al primer usuario para confirmar que la transferencia está completa.

12. Un método para retirar efectivo de un ATM que comprende: Recibir una solicitud en un primer formato por el titular de la cuenta para retirar efectivo del ATM; Recibir un número de teléfono celular del titular de la cuenta; Verificar en el modulo de procesamiento front end si la solicitud es aceptada o declinada con base en el número de teléfono celular y los fondos disponibles en la cuenta del titular; Transmitir el código temporal al titular de la cuenta; Recibir de la ATM una solicitud en un primer formato que incluye el código temporal, el número de teléfono celular del titular de la cuenta, y el código de identificación del usuario; Transmitir al servidor de la institución financiera una solicitud en un segundo formato para dispensar efectivo; y Recibir autorización de dicho servidor para retirar el efectivo.

13. El método de la reivindicación 12, en donde dicho primer formato es un mensaje ISO 8583 modificado con una parte fija y una parte variable y dicho segundo formato es un mensaje ISO 8583.

14. El método de la reivindicación 12, además comprende transmitir un mensaje de texto al titular de la cuenta para confirmar la transacción de dispensar efectivo.

15. Un método para procesamiento electrónico de compras en un punto de venta que comprende: Recibir en una interfase de aplicación de programa, un mensaje en un primer formato desde un punto de venta que incluye un número celular de usuario y un valor de compra; Convertir dicho mensaje en el primer formato en un mensaje en un segundo formato; En el modulo de procesamiento de front end, recibir dicho mensaje en un segundo formato y encontrar parámetros dentro de dicho mensaje en un segundo formato; Iniciar una rutina de interfase de voz en un módulo de interfase de voz; Realizar una llamada al usuario utilizando la rutina de interfase de voz y obteniendo autorización del usuario para la transacción de compra una vez el usuario ingrese su Numero Personal de Identificación; Transmitir un código temporal al punto de venta; Recibir, en una interfase de aplicación de programa, un segundo mensaje en un primer formato desde el punto de venta que incluya una solicitud de renovación de la transacción de compra, la solicitud renovada incluyendo el código temporal; y Autorizar la transacción de compra.

16. El método de la reivindicación 15, en donde dicho primer formato es un mensaje ISO 8583 modificado con una parte fija y una parte variable y dicho segundo formato es un mensaje ISO 8583.

17. Un método para procesamiento electrónico de desembolsos de nómina que comprende: Recibir autorización del empleador para pago de nómina con uno o dos tokens de seguridad; Verificar que la cuenta del empleador esté activa y que el empleador no haya excedido el número de autorizaciones; Recibir el pago de nómina solicitado en un primer formato; Convertir la solicitud en un segundo formato; Autorizar el pago de nómina si la cuenta del empleador tiene saldo suficiente y el número de autorizaciones no ha sido excedido; y Acreditar en la cuenta del empleado.

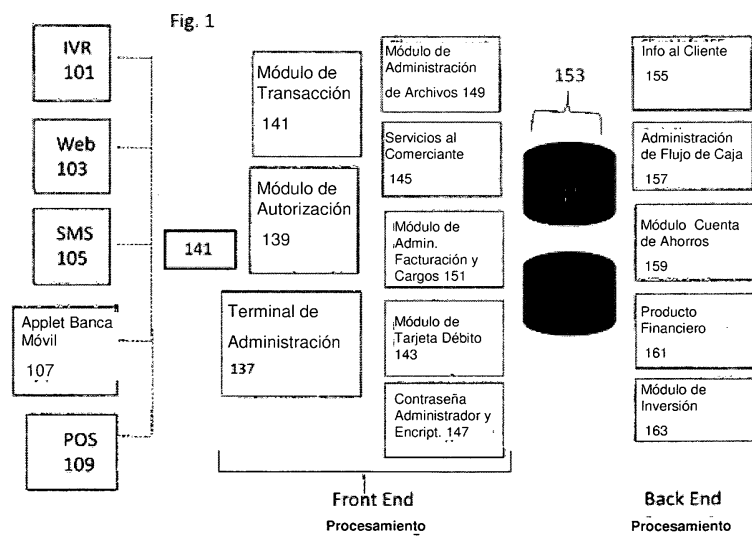
18. El método de la reivindicación 17, en donde dicho primer formato es un mensaje ISO 8583 modificado con una parte fija y una parte variable y dicho segundo formato es un mensaje ISO 8583.

19. Un método para el procesamiento electrónico de pagos a beneficiarios que comprende: Recibir un mensaje de un teléfono celular en un primer formato que incluye una solicitud de pago a un beneficiario, el mensaje incluye el número de teléfono celular de un solicitante, el código de identificación del solicitante, la identificación de un beneficiario, y una suma de pago; Convertir el mensaje en un segundo formato; Autorizar el pago si la cuenta del solicitante tiene saldo suficiente, un número de autorizaciones no es excedido, y el código de identificación es válido; y Acreditar en la cuenta del beneficiario.

20. El método de la reivindicación 19, en donde dicho primer formato es un mensaje ISO 8583 modificado con una parte fija y una parte variable y dicho segundo formato es un mensaje ISO 8583.

RESUMEN

[0071] Los sistemas y métodos de la presente invención incluyen una arquitectura de sistema integral que permite el acceso a instituciones financieras no bancarias (NFBIs) y bancos a través de dispositivos en punto de venta y teléfonos móviles, por ejemplo. La presente invención involucra el uso de un estándar ISO 8583 modificado para permitir a los usuarios hacer interfase con un sistema de procesamiento de front end directamente desde los dispositivos no tradicionales. La presente invención también permite banca móvil con los NBFIs a través del uso de una aplicación que reside en un teléfono móvil de un usuario, que permite el encapsulamiento de información del usuario como XML, por ejemplo, y la transmisión de ellos sobre http mientras cumple con el estándar ISO 8583, y además permite la encriptación de ciertos datos de usuario, sin que tenga que recurrir al acceso a la página web de banca móvil. En un aspecto de la invención, una aplicación POS puede ejecutarse en la parte superior de PCI para permitir a los usuarios hacer compras utilizando fondos pre-depositados en una cuenta NBFIs.



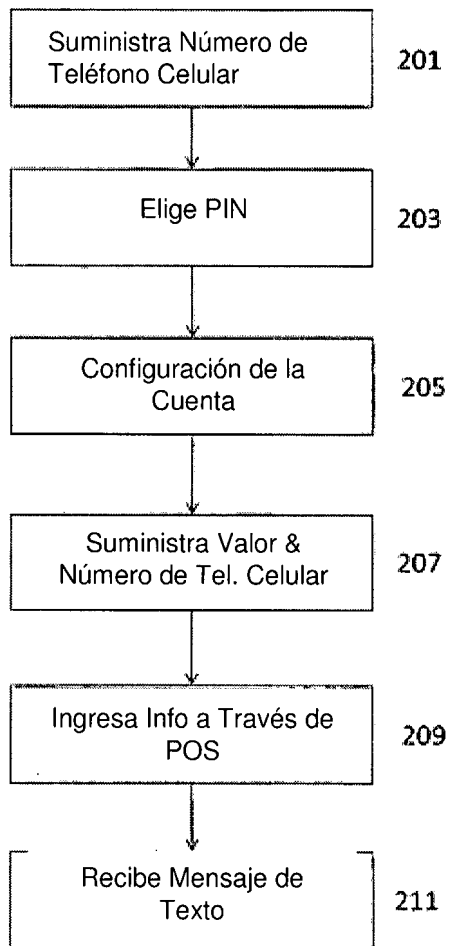


Fig. 2

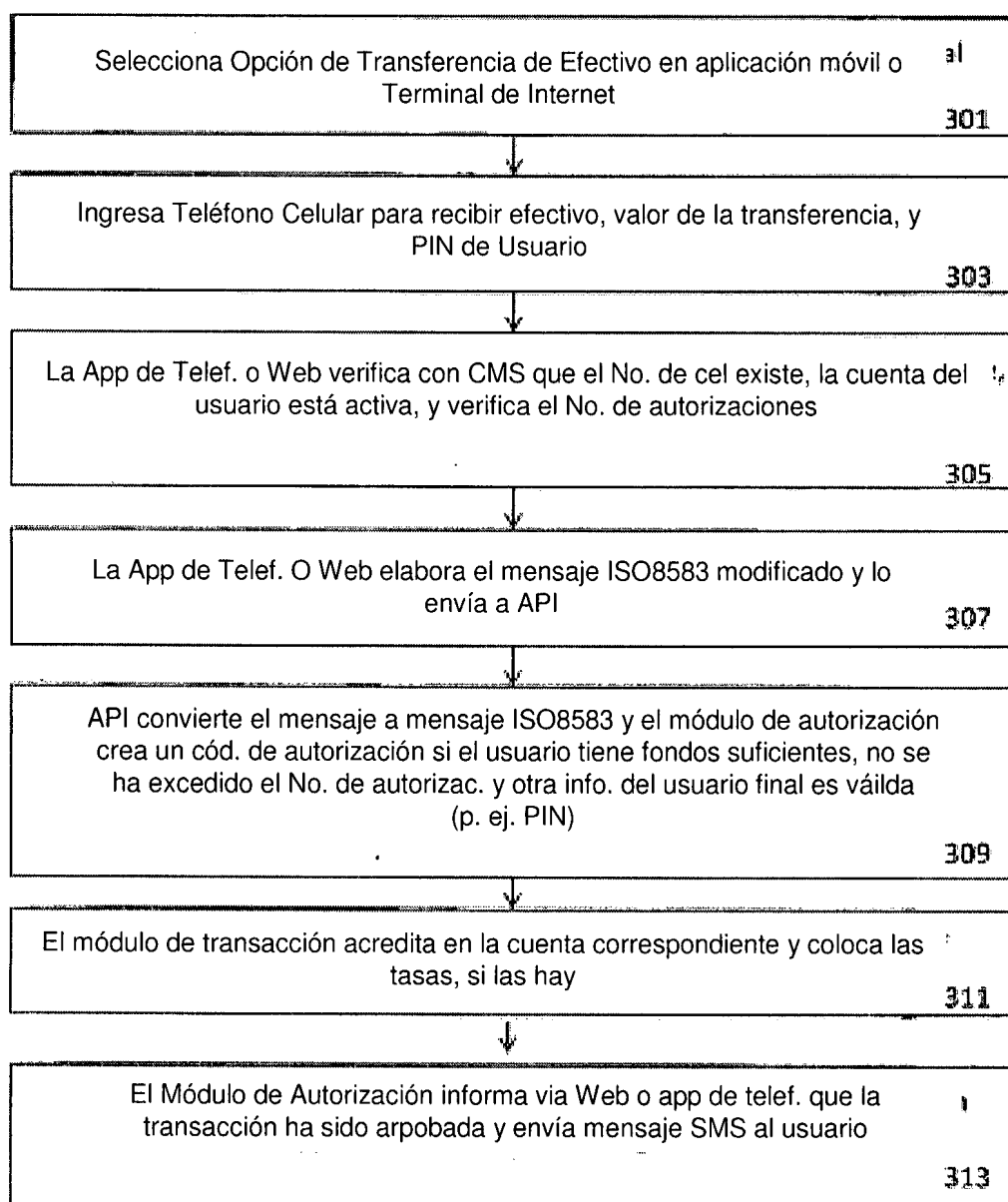


Fig. 3

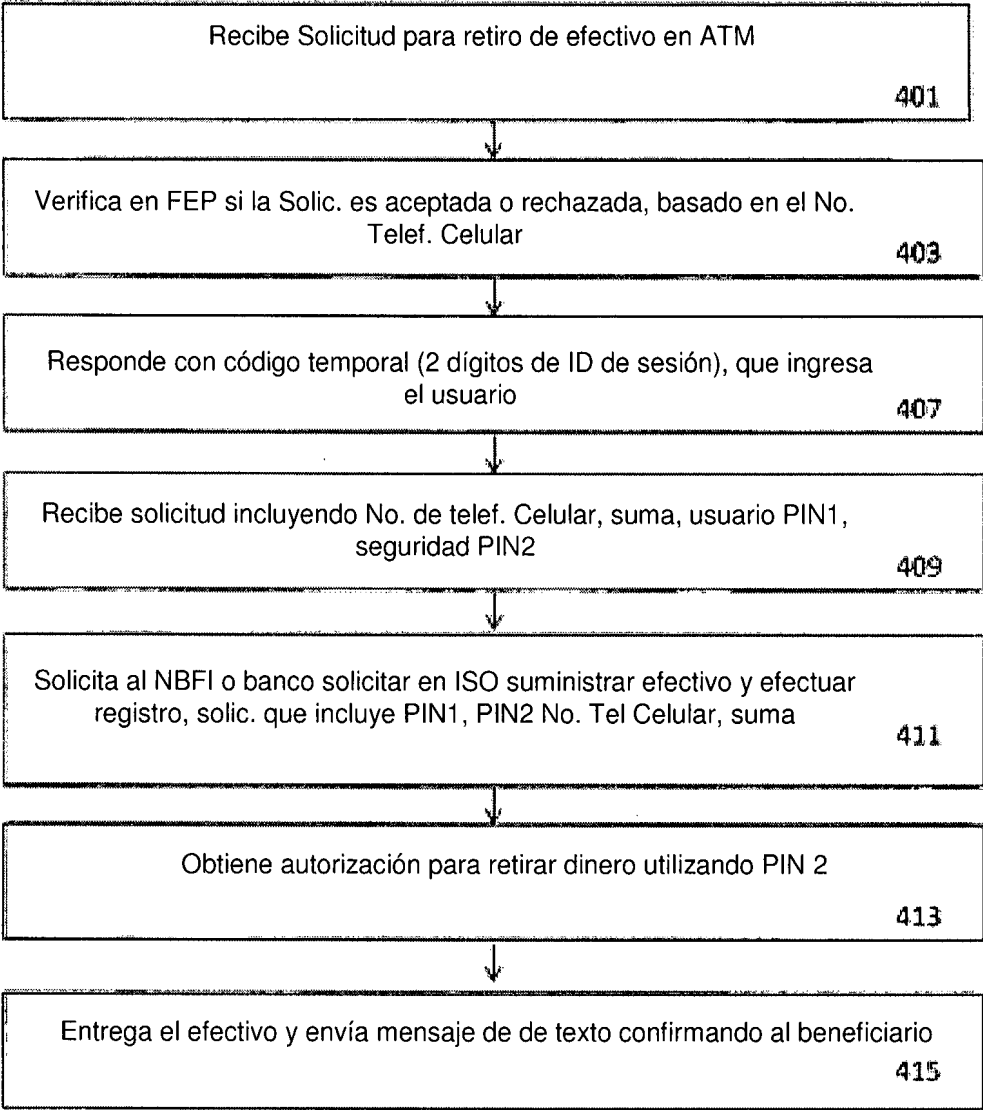


Fig. 4

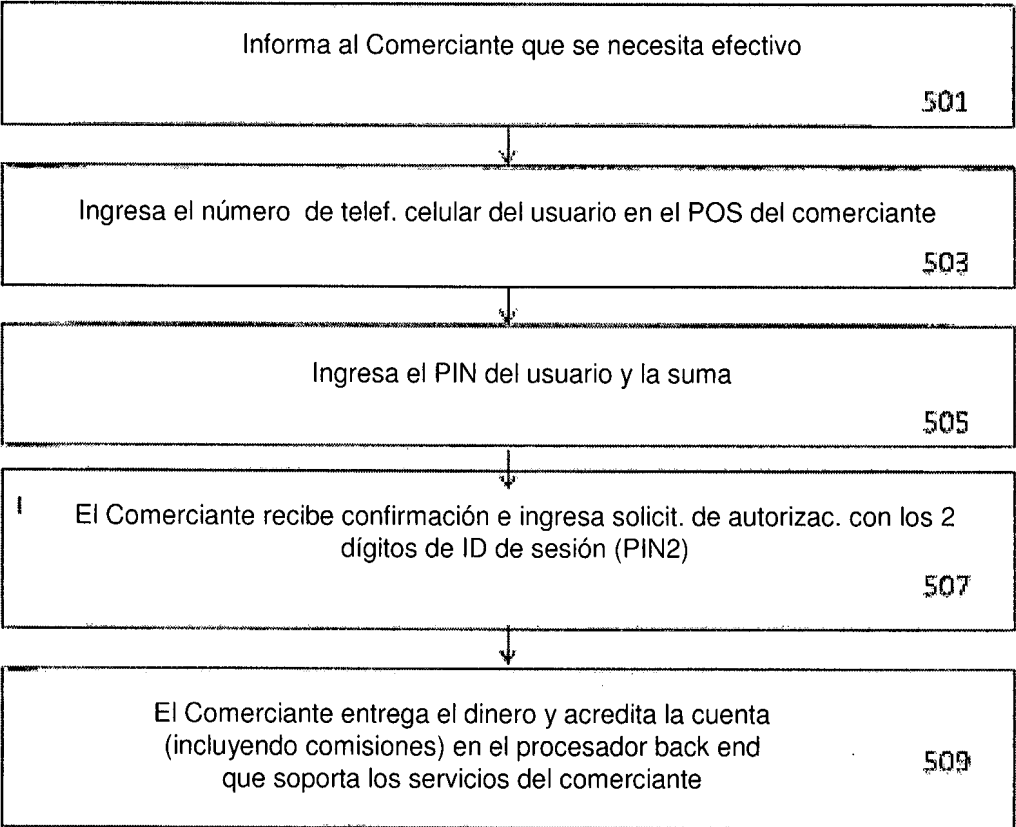


Fig. 5

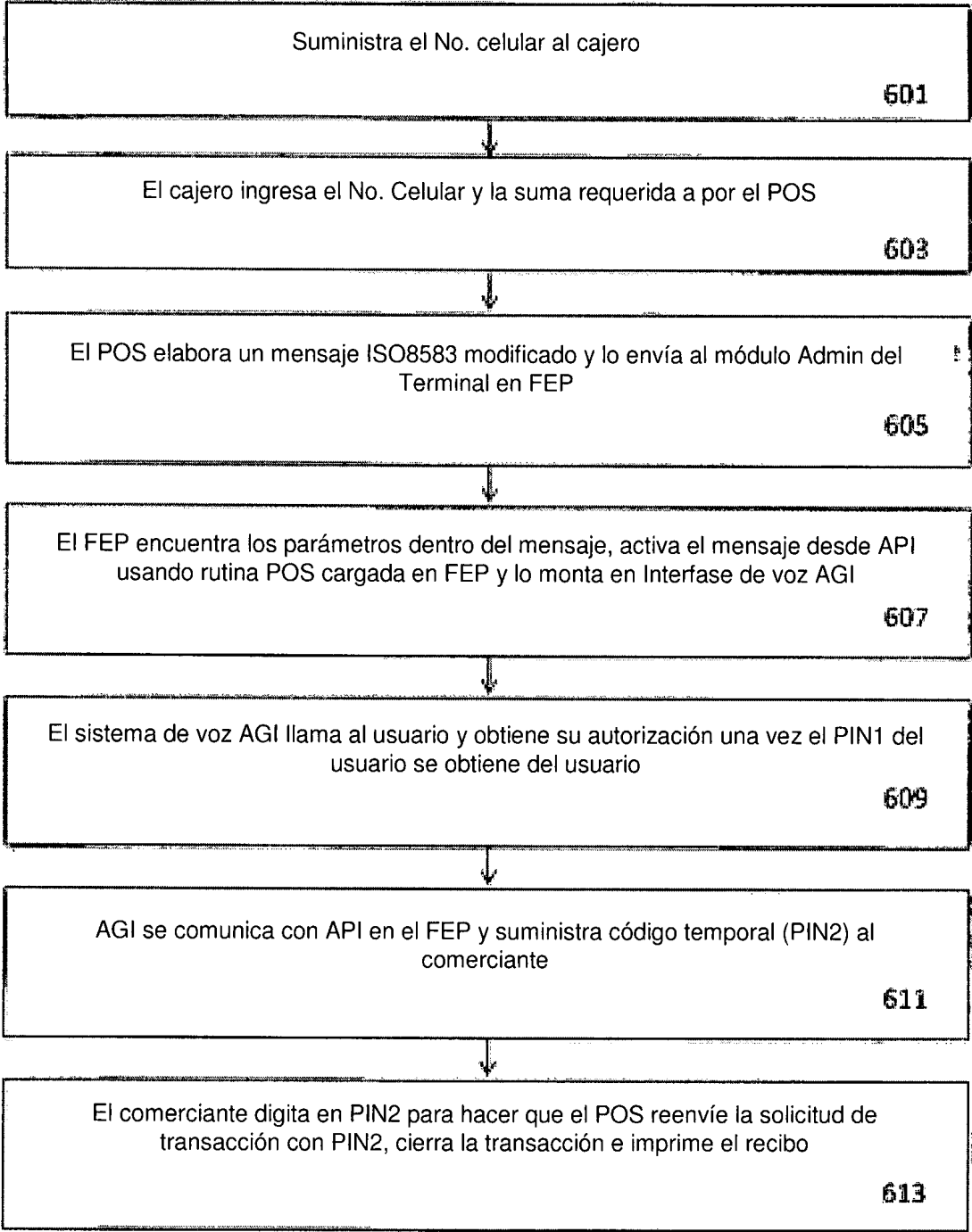


Fig. 6

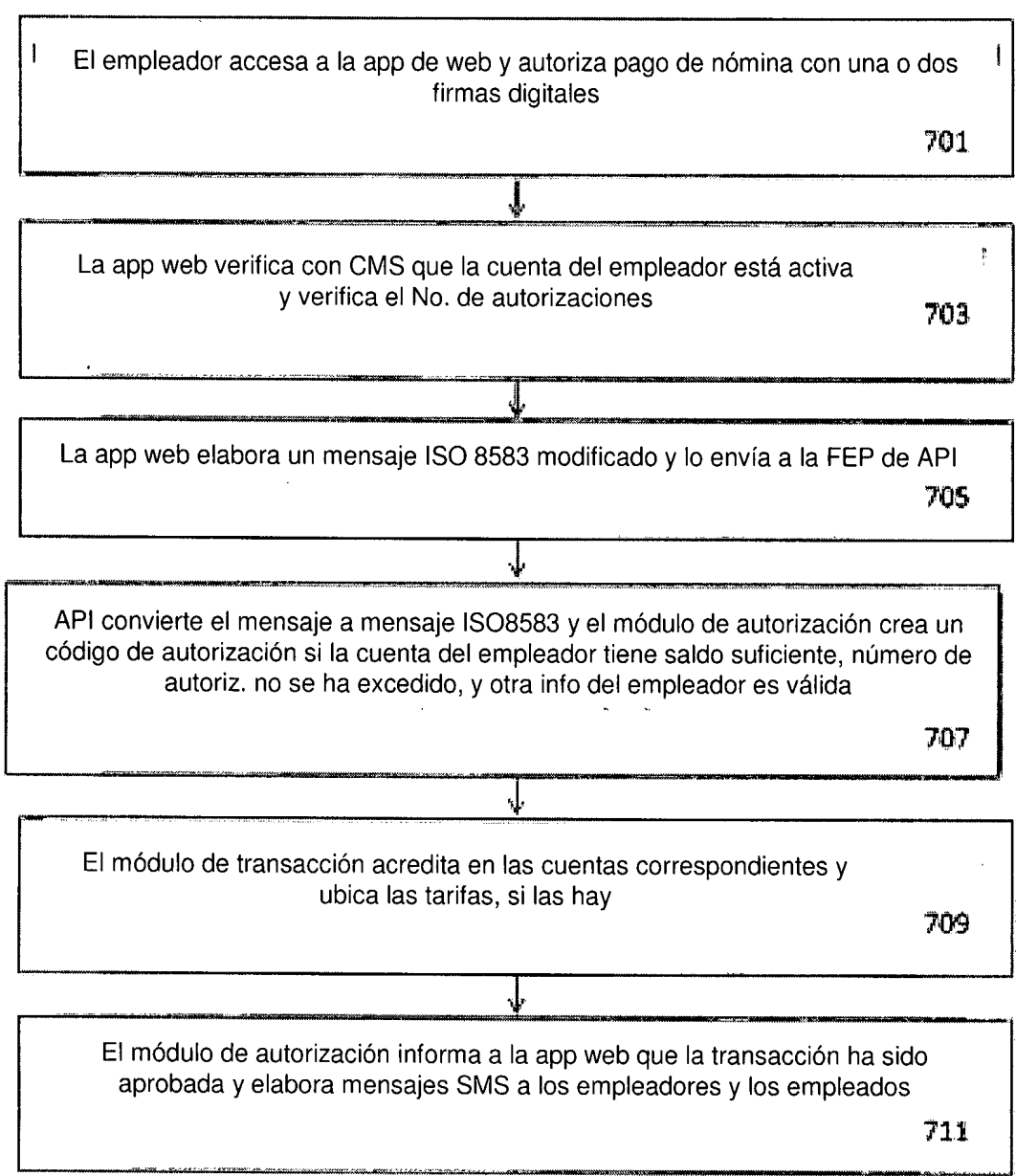


Fig. 7

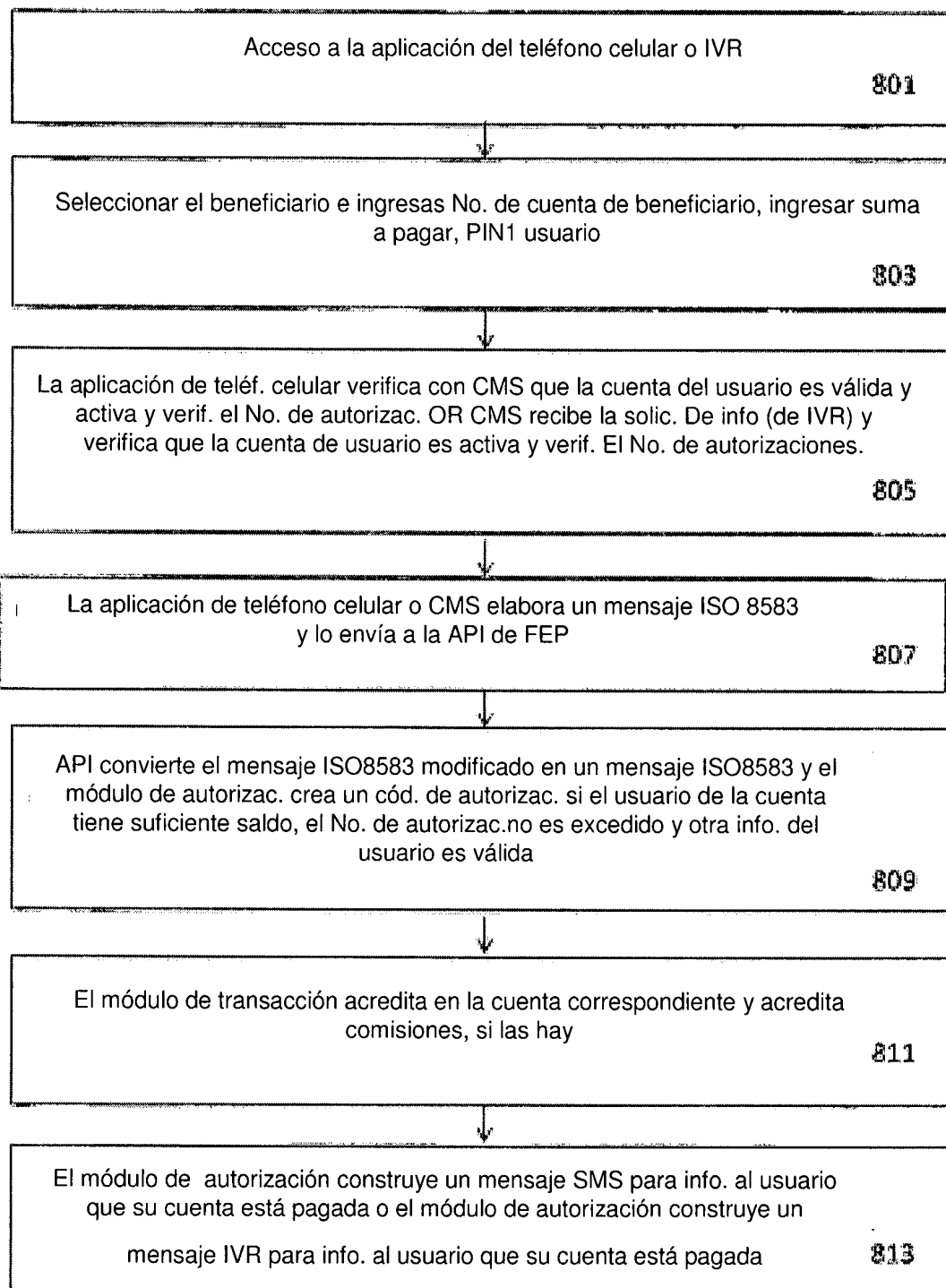


Fig. 8

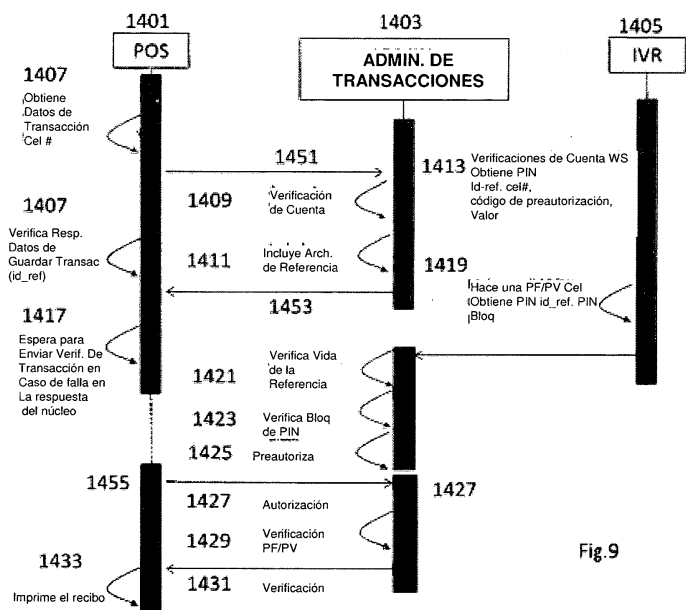


Fig.9

SYSTEM AND METHOD FOR CONDUCTING FINANCIAL TRANSACTIONS**FIELD OF THE INVENTION**

[0001] The present invention relates to data processing systems and methods for conducting financial transactions over a network. More particularly, the present invention relates to integrated systems and methods which provide secure access to capital and that enable financial transactions by using wireless technology, such as mobile devices.

BACKGROUND OF THE INVENTION

[0002] Businesses dedicated to cashing checks and bill payment on behalf of others are striving in the United States and other parts of the world as well. Low income families are practically forced to use these services due to high fees charged by banks for keeping a low balance in an account and due to high initial deposit requirements to open an account. Migrant workers are also forced to use these services as banks do not allow an individual to open an account without providing an address in the U.S. Overall, a large percentage of the population in the U.S. has no access to capital or financial services through banks. This is something that check cashing companies take advantage of by making short-term loans at a very high interest. These conditions have created a problem that essentially jeopardizes the safety of individuals that always carry cash. These conditions also potentially create a problem in that they may affect a taxing authority's ability to collect taxes for transactions that cannot be traced.

[0003] Non-bank financial institutions ("NBFIs") have become an efficient alternative to banks in terms of providing financial services to individuals with limited wealth or economic resources. The service of accepting monetary deposits from the public is typically regulated or controlled by state or federal law and regulations and these NBFIs are not exempt from such laws or regulations. At a global level, these NBFIs allow wider access to financial services, especially to individuals that reside far from big cities. In fact, one of the main aspects that limit worldwide ease of access to banks is the scarcity of branches that offer client services, etc. Not surprisingly, one of the goals of NBFIs is to increase the number of locations where clients can be serviced by increasing the number of non-traditional channels, authorizing banking institutions to offer financial services through the NBFIs, such as stores, supermarkets, etc. While, NBFIs constitute a tool against financial exclusion, there is still a need for a system to allow easier access to capital or financial services through NBFIs and banks.

SUMMARY OF THE INVENTION

[0004] The following presents a simplified summary of the invention in order to provide a basic understanding of some aspects of the invention. This summary is not an extensive overview of the invention. It is intended to neither identify key or critical elements of the invention nor delineate the scope of the invention. Its sole purpose is to present some concepts of

the invention in a simplified form as a prelude to the more detailed description that is presented later.

[0005] The present invention includes a comprehensive system architecture that enables access to NBFIs (or banks) through point-of-sale devices and mobile telephones, for example. In one embodiment of the present invention, the ISO 8583 standard is expanded so as to allow users to interface with a front end processing system directly from non-traditional devices.

[0006] In another embodiment of the present invention, mobile banking with the NBFIs or banks can be achieved through use of an application residing in a user's mobile telephone, which allows the encapsulation of user information as XML, for example, and the transmission of those over http while complying with the aforementioned ISO 8583 expansion, and further allowing encryption of certain user data. In yet another embodiment of the present invention, a POS application may run on top of the PCI standard to enable users to make purchases using funds pre-deposited in an NBFIs account. To achieve this, the POS application may initiate a session with the NBFIs or bank and use an encrypted message obtained through that first session to encrypt information as part of a second session which will then be used to finalize the transaction while the first session expires.

[0007] The following description and the annexed drawings set forth in detail certain illustrative aspects of the invention. These aspects are indicative, however, of but a few of the various ways in which the principles of the invention may be employed and the present invention is intended to include all such aspects and their equivalents. Other advantages and novel features of the invention will become apparent from the following detailed description of the invention when considered in conjunction with the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] Fig. 1 illustrates a financial transaction architecture in accordance with one embodiment of the present invention;

[0009] Fig. 2 illustrates a method for setting up a user account in accordance with one embodiment of the present invention;

[0010] Fig. 3 illustrates a method for electronic transfer of cash to another account in accordance with one embodiment of the present invention;

[0011] Fig. 4 illustrates a method for obtaining a one-time use PIN for use an ATM in accordance with one embodiment of the present invention;

[0012] Fig. 5 illustrates a method for electronic processing of cash withdrawal through use of POS in accordance with one embodiment of the present invention;

[0013] Fig. 6 illustrates a method for electronic processing of purchases at a merchant's location in accordance with one embodiment of the present invention;

[0014] Fig. 7 illustrates a method for electronic processing of payroll disbursement in accordance with a first embodiment of the present invention;

[0015] Fig. 8 illustrates a method for electronic processing of payments to payees in accordance with a second embodiment of the present invention; and

[0016] Fig. 9 illustrates a flow of transactions related to the electronic processing of purchases or cash withdrawals in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

[0017] The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art.

[0018] As will be appreciated by those skilled in the art, portions of the present invention may be embodied as a method, data processing system, or computer program product. Accordingly, these portions of the present invention may take the form of an entirely hardware embodiment, an entirely software embodiment, or an embodiment combining software and hardware aspects. Furthermore, portions of the present invention may be implemented as a computer program product on a computer-usable storage medium having computer readable program code on the medium. Any suitable computer readable medium may be utilized including, but not limited to, static and dynamic storage devices, hard disks, optical storage devices, and magnetic storage devices.

[0019] The present invention is described below with reference to illustrations of methods, systems, and computer program products according to embodiments of the invention. It will be understood that blocks of the illustrations, and combinations of blocks in the illustrations, can be implemented by computer program instructions, hardware devices, or a combination of both. These computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a particular machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, implement the functions specified in the block or blocks.

Transactions Implemented Through Modified ISO 8583

[0020] Fig. 1 illustrates an exemplary architecture of the system of the present invention in accordance with one embodiment. The system includes a number of front end processing modules that interface with remote devices through an ISO 8583 messaging interface 141 modified in accordance with the present invention. Although ISO 8583 defines a common

standard, it is not typically used directly by financial transactional systems or networks. Instead, each network adapts the standard for its own use with custom fields and custom usages.

[0021] The placement of fields in different versions of the standard varies. For example, the currency elements of the 1987 and 1993 versions of the ISO 8583 standard are no longer used in the 2003 version, which holds currency as a sub-element of any financial amount element. As of the time of this writing, ISO 8583:2003 has yet to achieve wide acceptance.

[0022] An ISO 8583 message is made of the following parts:

Message type indicator (MTI)

One or more bitmaps, indicating which data elements are present

Data elements, the fields of the message.

[0023] The remote devices or systems that can access the system of the present invention include an electronic cash register (ECR) (not illustrated); an Interactive Voice Response (IVR) module 101, a point-of-sale device (POS) 109, which may communicate with a near field communications reader (NFC) to read information from a credit card or mobile device, for example; a computing device with access to the Internet (Web) 103; a cell phone with an application for mobile banking (MB) 107; and a remote device capable of receiving SMS messages (SMS) 105. Remote devices 101, 103, 107, and 109, may communicate with the API 141 through the Internet or Access point Network (APN) circuitry. Some of these are "smart" remote devices that can assemble a modified ISO 8583 message and send it to the API 141. For other devices with limited capabilities, a client management service (CMS) (not illustrated) may be used for assembling a modified ISO 8583 message and forward the corresponding modified ISO 8583 message to the API 141. For example, The CMS verifies information received from the devices before assembling the modified ISO 8583 message. In general, the CMS verifies that a particular cell phone number exists, as in one embodiment of the present invention a user's cell phone number is used as the account number, verifies that the user account is active, and checks that the maximum number of allowances (e.g., number of transactions allowed per month, day, etc.) has not been exceeded. The information verified and provided by the CMS may be used in assembling modified ISO 8583 messages. The CMS may then send the modified ISO 8583 message to the AP 141 or it can forward verification parameters to a smart device for assembly of the ISO 8583 modified message.

[0024] As mentioned, the remote devices can be used for exchanging modified ISO 8583 messages with the API 141, which resides in a switching server. Other components of the switching server may include a switch module, an ATM module, an ACH module, and a module for interfacing with other networks. One of the functions of the API 141 is to convert the modified ISO 8583 messages into standard ISO 8583 messages. Another function includes passing those ISO 8583 messages to other modules which are part of the system of the present

invention, for example the terminal administration module 137 or the authorization module 139. When the API 141 conducts messaging with those modules, for example, the financial transaction is referred to as a closed loop transaction. When the API 141 exchanges messages with a switch module, the ACH module or the other network module in the switch server, the messages from the API 141 leave the network architecture illustrated in Fig. 1, and as such, the transactions involving that type of messaging are referred to as open loop transactions, as would be understood by a person of ordinary skill in the art.

[0025] The system of the present invention may include front end processing modules (FEP). In one embodiment of the present invention, the FEP includes acquirer modules (i.e., modules 137-141 that acquire instructions or commands from the remote devices) and processing modules (i.e., modules 143-151 that execute instructions for reading or writing information into the database 153). The FEP may be implemented in a server separate from the switching server. In one embodiment of the present invention, the acquirer and processing modules can be implemented as separate virtual machines running on the same server.

[0026] The FEP acquirer modules may include a terminal administration module 137, an authorization module 139 and a transaction module 141. The terminal administration module 137 is used to process requests from POS and ECR devices. These requests may include identification of the POS or ECR, origination account information, destination account information, and amount of transaction and of transaction fee.

[0027] In one embodiment, transaction requests from remote devices other than a POS or ECR may be passed by the API 141 directly onto the authorization module 139. The authorization module 139 verifies whether the account to be debited has enough balance to complete the transaction, that the PIN entered for user authentication (e.g., PIN1) matches the PIN stored in the database 153, and verifies that the number of allowance are met. The PIN is recreated internally by the password and cryptography module 147, which may be implemented as a hardware-based cryptography card. Upon authorization, the module 139 issues an authorization code. In one embodiment, the last two digits of the authorization code may be used as a temporary/one-time use code (i.e., PIN2) to conduct ATM transactions or purchase transactions.

[0028] The authorization code is passed on to the transaction module 141, which generates instructions to write credits to accounts, post debit to accounts, as well as fees. For example, if the transaction requested is for a purchase, the transaction module 141 instructs the merchant services module 145 to write a credit to the merchant account in the database 153, instructs the debit card module 143 to write a debit to the user's account in the database 153, and instructs the billing and administrative feed module 151 to post a fee associated with the transaction. As transactions are completed, the file management module 149 keeps a record of the transactions processed (e.g., time of transaction, etc.). 141

[0029] In another aspect of the present invention, the database 153 is shared by the FEP modules and the back end processing (BEP). In the illustrated embodiment, the BEP modules include client information module 155, cash flow management module 157, savings account module 159, financial product module 161, and investment module 163. These BEP modules are associated with traditional banking functions. In one embodiment, they may be implemented as modules used to create reports containing basic client information (155), information about a client's cash flow management (157), information regarding a client's savings (159), information about financial products used by a client (161), and information about a client's investments (163).

[0030] One of the advantages of the present invention is that users of the system can activate or create accounts without the need to undergo all the formalities imposed under a traditional banking model. Consequently, some of the more traditional banking functions associated with the BEP processing may not be necessary for a user of the present invention. For example, in a preferred embodiment, a user may go to a store or merchant that operates a POS to open an account with an NBFi or bank, or to open with an NBFi or bank a prepaid debit account having a limit in terms of number of transactions and cash limit as well as means for reporting money laundering to authorities. The system still allows these transactions to take place on site. The present invention does not inhibit the KYC (Know Your Client) process if mandatory and the BEP allows processing of transactions that involve face to face contact for account creation or the simplified account creation process of the preferred embodiment of the present invention. The user or new client would hand cash to the merchant to deposit into an account associated with the mobile telephone number of that client. Using the IVR interface 101, a client of an NBFi or bank implementing the system of the present invention may dial in to the system to find out balance information, authorize transactions, etc. Using the web interface, a user of the system, for example an employer, may log in to the system and authorize payroll payments by transferring funds from an NBFi or bank, for example, to an employee account. Also, the system of the present invention may send text messages (e.g., SMS) to confirm that transactions have been completed. These exemplary transactions will be discussed below in more detail.

[0031] Fig. 2 illustrates one type of transaction that may be performed through use of a POS in which a new client of the NBFi or bank using the present invention can activate an account at a merchant's location. The merchant is appointed as an Independent Correspondent or authorized store by the bank or NBFi. A client can make an initial deposit at a selected location, for example at any of the associated stores or Independent Correspondents. In step 201 a merchant would enter into the POS 109, for example, the cell phone number associated with the new client. The client would wait until the system calls him/her to verify the identification of the owner of the cell phone. The client would then choose a PIN (step 203) and this PIN is entered into the POS connection to the FEP to approve a requested authorization by the POS device, which is part of account setup step 205, to reinitiate the completion of the request by entering a

temporary code provided to the Merchant by the system, enabling the transaction to go forward with all included parameters enabled by the exchange of information between the account holder (via the Telephone), the merchant providing invoicing and allowing electronic payment with confidentiality of information, and the validation and decision by the consumer to complete the payment, and notification of the decision with the temporary code to Merchant's POS operator. The POS will then get confirmation and additional parameters to verify the validity and information about owner of the account. The system of the present invention would then setup the account in step 205. Upon receipt of cash and upon account activation methods by NBFi or Bank, the merchant may enter the account holder's cell phone number into the POS 109 in steps 207 and 209 to credit the account upon receiving cash for "loading" the account. After the account has been funded, the client receives a text message via a Short Message System (SMS) confirmation of the transaction in his cell phone through an SMS message (on top of previous amount to debit from his Account by IVR), for example (step 211).

[0032] Fig. 3 illustrates a method for transferring cash from one NBFi or bank account holder to another. In step 301 the user selects the cash transfer option from a menu displayed by the MB 109 or Web 107, for example after the MB 109 or Web 107 recognizes a particular transfer or account, the user then enters the cell phone number associated with the other account holder (step 303) or debit card number at destination account as well as the amount to be transferred and the user authentication PIN (i.e., PIN 1). The application installed in the terminal Web 107 or cell phone MB 109 then communicates with the CMS to obtain verification that the cell phone numbers exist (enabled by network signaling and data base at CMS with registered numbers and associated account), that the accounts are active and checks the total number of allowances for the transferor (step 305). In step 307 the web or phone application builds a modified ISO 8583 message based on the information provided by the CMS and sends it to the API 141.

[0033] In step 309 the API 141 converts the received message from modified ISO 8583 to standard ISO 8583 and the authorization module 139 issues an authorization code if the user account has sufficient funds, the number of allowances is not exceeded, and other end-user information, such as the PIN, is validated. In step 311 the transaction module 141 communicates with merchant services module 145 and debit card module 143 and instructs these modules to post the appropriate debit and credit in the database 153 with respect to the accounts involved in the transaction. The transaction module also instructs the module 151 to calculate and post the fee associated with the transaction, if any. In step 313 the authorization module informs the web or phone application residing in Web 107 or MB 109 that the transaction has been approved and also builds a message that is sent to the user through the SMS interface 111. The transferor and the transferee receive a text message confirmation (e.g., SMS) of the transfer.

[0034] Fig. 4 illustrates a method for retrieving cash from an NBTI or bank authorized ATM in accordance with one embodiment of the present invention. This transaction is prepared by the Client (end User) in advance for a specific amount using IVR functionality. In step 401 the system receives a request for withdrawing cash at an ATM, for example a franchised ATM to brand or enable an ATM Network with the present system's non-card request. If the request is made at the ATM, the request may be triggered by a soft key or a button pressed by the user to indicate that the user seeks to withdraw cash without using an ATM card. The request may be accompanied by the user's cell phone number. Before sending the request to the API 141, the ATM communicates with the CMS Database to determine whether the user account is valid, etc. In step 403, the ATM sends the request to the authorization module 139 in the FEP through an ATM interface (ATM HUB Application for switching the transaction to FEP using the standard ISO8583 messaging) and the FEP determines whether the request is accepted or declined (according to the parameters set by user requests when preparing the ATM withdrawal request through the IVR), based on whether the account associated with the cell phone number is active as a first check to approve/decline before proceeding. If the request is not accepted, the system generates a reply with a message denying the request for withdrawal. For example, the user may receive a text message (or the ATM may display such message) that the request has been denied. In step 407, if the request is accepted, the user may receive a text message with a temporary authorization code to enter (PIN2). In one embodiment, this temporary code may be the last two digits of an authorization code generated by the authorization module 139 in response to the original request.

[0035] In step 409, the user may enter the temporary code along with a user PIN (PIN1) and amount to be withdrawn. In step 411, the ATM requests the licensed NBTI or bank to request an ISO8583 authorization to provide cash. While this request is based on ISO8583, the communications between the ATM and the FEP are based on the modified ISO8583 of the present invention. In step 413, the issuer (licensed bank or NBTI) authorizes the cash withdrawal based on PIN2 as well as additional parameters. In step 415, the ATM receives and processes information for authorizing the transaction, it dispenses the cash, and an SMS message is sent to the user confirming the transaction.

[0036] Fig. 5 illustrates at a high level a method for the retrieval of cash at a merchant location, for example. A more specific method may be implemented by using a method similar to the method described with respect to Fig.4 except that the user interface would be a POS instead of an ATM. Referring to Fig.5, in step 501 a user requests the merchant for cash. In step 503 the merchant enters the end- at the POS. In step 505 the merchant enters the user's cell phone number, amount of withdrawals, and PIN1 into the POS application. In step 507 the merchant enters request for authorization with PIN2 (last two digits of session ID to be included in a POS transaction to complete the ISO8583 modified request or complete the authorization) receives text with confirmation that it can tender cash to the user, assuming the user has funds.

In step 509 the merchant tenders cash and the merchant's account gets credited at the backend processor supporting the merchant's services.

[0037] Fig.6 illustrates a method for purchasing goods at a merchant's location. After the cashier has obtained the total amount owed for the sale of goods, the user provides a cell phone number associated with the NBF1 or bank account to the cashier (step 601). At step 603 the cashier enters, through an ECR (or a POS device), the cell phone number and the amount owed into the system. In step 605, the ECR builds a modified ISO8583 message requesting authorization and sends it to the Terminal Administration Module 137 in the FEP. In one embodiment, the modified ISO 8583 message is built after verification of certain user data is received from CMS, as described above. In step 607 the FEP finds the variable part parameters in the message, triggers a message from the API 141 using a POS/ECR routine loaded on the FEP, and starts the voice interface routine (AGI, which stands for Asterisk Graphics Interface). The AGI voice system makes a call to the user and obtains user authorization once user enters his/her PIN number associated with the account (step 609). In step 611 the AGI communicates with the API at the FEP and provides a temporary code for user. In one embodiment, the temporary code may be the last two digits of an authorization code issued by the authorization module 139. In step 613, the merchant keys in the temporary code provided by the user to force the ECR/POS to restructure the modified ISO 8583 message, send the message to the API 137, and close the transaction.

[0038] Fig.7 illustrates a method that may be used by an employer to make payroll payments to its employees. In step 701 the employer logs into its account through a web interface and then authorizes the payroll disbursement. This payment may be a transfer from one NBF1 or bank account into one or more NBF1 or bank accounts. In step 703 a web application requests that the CMS Database verify that the employer account is active, for example, and that the number of allowances associated with the employer account has not been exceeded. Upon verification, in step 705 the web application builds a modified ISO8583 message and communicates the message to the API 141. In step 707, the API 141 converts the message to a standard ISO8583 message, and the authorization module 139 issues an authorization code if the employer account has sufficient balance, the number of allowances is not exceeded, and other employer information is valid. In step 709 the transaction module 141 instructs the corresponding processing modules in the FEP to write credits and debits to the employer and employee accounts, together with the associated fees. In step 711 authorization module informs the web application that the transactions have been approved and builds SMS messages that are sent to the employees and employer to confirm disbursements.

[0039] Fig. 8 illustrates a method to make payments to a payee (e.g., a utility company). In step 801 a user accesses a cell phone application or dials into an IVR system for mobile banking. In step 803 the user accesses a list of payees displayed on the cell phone or communicated to the

user through the IVR interface. The user selects the payee and enters the payee account information, the amount of payment, and a PIN.

[0040] In step 805 the CMS Database verifies that the user account is active and valid and verifies that the number of allowances has not been exceeded. If the user is accessing the system through the MB interface 107, the cell phone application sends the request for verification to the CMS and does not build a modified ISO 8583 message until the CMS verifies the user account. If the user is accessing the system through the IVR interface 101, the CMS receives the request for verification but does not need to respond to the IVR interface 101.

[0041] In step 807, the cell phone application builds the modified ISO 8583 message to request the payment transaction to the system when the user requests such transaction through the MB 107. Alternatively, the CMS with a program script suited for building the modified ISO 8583 message when the user requests the transaction through the IVR 101. Then, either the MB 107 or the CMS sends the modified ISO 8583 message to the API 141.

[0042] In step 809 the API 141 converts the modified ISO 8583 message to a standard ISO 8583 message and forwards the converted message, together with parameters in the variable part of the modified ISO 8583 message, to the authorization module 139. The authorization module 139 then issues an authorization code if the user account has sufficient balance, the number of allowances has not been exceeded, and other user information is valid (e.g., PIN). In step 811 the transaction module 141 instructs the corresponding processing modules in the FEP to write a credit and debit to the corresponding accounts, together with the associated fees. In step 813, the authorization module 139 builds an SMS message to inform the user that the bill has been paid. Alternatively, the authorization module 139 builds an IVR message to inform the user through the IVR interface 101 that the bill has been paid.

[0043] As mentioned, these transactions take place without the user making use of the Internet as he or she would have to do with conventional mobile banking. The interface between the user and the system is based on a variant of the ISO 8583 as explained above. The formatting of the modified ISO 8583 message will be explained below. The messages exchanged between the server interfacing with the users and the FEP are also based on the standard ISO8583.

[0044] All of the above transactions may be metered in a Primary CMS Data Base and other modules to build the message using a specific script connected with every interface using an XML library written for the particular use, in accordance with one embodiment of the present invention. Such Data Base serves to control user activity (including fractioning transaction to hide laundering) and limits exposure or abusive usage by the clients and it may be considered a fraud prevention mechanism. Such Database is connected to the voice components, messaging, web log in and mobile banking log in. It measures the overall activity of the user accounts regardless of the interface selected by the user. For example, on the voice processing system it

allows routing when a cell phone number associated to an account exists and blocks the usage when the account is flagged for any reason or it has been deactivated or doesn't exist. That call flow and information exchange may be controlled by a script managing the voice switching capability and all other interfaces exchanging the information via XML messages.

Modified ISO 8583 Format

[0045] Financial industry services include the exchange of electronic messages relating to financial transactions. An international effort was carried out by the International Standard Organization (ISO) with a main goal of defining a unique message structure to be used by all financial institutions around the world. ISO 8583 is the name of the international standard for financial transaction card originated messages. It specifically defines a unique data structure for interchanging messages between heterogeneous financial networks. Specifically, the standard specifies a common interface by which financial transaction card originated messages may be interchanged. It specifies structure, format and content, data elements and values. One advantage of the present invention is that it allows users to conduct financial transactions, for example purchases, without the need for a credit or debit card by converting modified ISO 8583 messages so that the financial network "sees" the cardless transaction as a credit or a debit transaction in full compliance of mandatory parameters.

[0046] ISO8583 messaging structures have a series of fields where transactional related data are stored. These fields are referred to as Bitmaps. The combination of distinct bitmaps is what makes up financial transactions that could be processed by a financial institution.

[0047] The ISO8583 standard is only the main sketch to follow by a financial entity in order to implement transactional units. The application specification may remain at private level. Application designers have complete design freedom, within the overall ISO 8583 constraint, so that messages are convertible to the ISO 8583 interface format so that international interchange may take place. The idea is that financial application developers are free to implement whatever is needed if and only if their messaging interfaces can be translated to ISO8583 specifications in order to promote international interchange.

[0048] The present invention leverages the flexibility of the ISO 8583 by implementing a common messaging interface focusing on the data to be interchanged rather than the complexity of denoting and declaring ISO 8583 bitmap schemes on the message. This feature is referred to herein as the Fixed Part, Variable Part Messaging Frames, interface. One of the benefits of this modified ISO 8583 interface is to ease transactional communication between third-party financial applications and the conventional back end processors which require conversion to the ISO8583 standard.

Fixed Part Variable Part Data Structures

[0049] In one embodiment of the present invention, data interchange between the front end modules and the end-user applications used to interface with the NBFi or bank are based on the use of the Fixed Part Variable Part Data Structures. According to this, data for transactions is put together in specific frames where every piece of data has a specific position in the frame.

[0050] The Fixed Part / Variable Part Frames are based on ISO 8583 premises. The first section of a communication frame from this implementation is referred herein as the Fixed Part and it contains all the shared information belonging to all the transactions in the system, for example, the time when the transaction was executed, the transaction code, the answer code, and others. The second section of the frame is referred herein as the Variable Part and it permits sending specific data depending on the transaction that will be executed. For example, whether the transaction that will be executed is Account Balance, then in the Variable Part of the modified ISO 8585 message basic information about the user will be sent. The Variable Part section also enables communication with non-traditional banking terminals such as mobile phones and POS devices. In one embodiment, the Fixed Part frame includes 250 characters while the Variable Part is variable in length.

[0051] The Fixed part structure may be defined as follows:

DESCRIPTION	I/O	TYPE	LENGTH	Decimals	From	To	Values/Constraints
ApplicationCode	O	A	2		1	2	Fixed value = CS : Indicates to FEP a transaction from NBFi OR BANK'S LICENSED OPERATOR

DESCRIPTION	I/O	TYPE	LENGTH	Decimals	From	To	Values/Constraints
TransactionCode	O	A	6		3	8	Alphanumeric indicator who defines codes to be interpreted by Core and corresponds to a specific transaction to execute This Field has the following structure: XXYYZZ XX code to indicate type of transaction. YY code to indicate the type of account who originates the transaction ZZ code to indicate type of the destination account.
TellerCode	O	A	9		9	17	000000000 This field may be filled with nine zeros.
Office Code	O	A	3		18	20	000 This field may be filled with three zeros
Date of Transaction	O	N	8	0	21	28	YYYYMMDD Example: 20090122 corresponds to January 22 of 2009.

DESCRIPTION	I/O	TYPE	LENGTH	Decimals	From	To	Values/Constraints
Time of Transaction	O	N	6	0	29	34	HHMMSS Example: 142510 corresponds to 14 hours 25 minutes 10 seconds
Effective date of transaction	O	N	8	0	35	42	YYYYMMDD This field has to take the same value of the Date of Transaction field in a request.
ChannelCode	O	A	3		43	45	Fixed value = IVR
SwitchCode	O	N	4	0	46	49	Numeric code that indentifies the actions to be followed in the Transactional Core
Device	O	A	2		50	51	Fixed value = 02(Value changed)
CorrelativeNumber	O	N	12	0	52	63	Represents a counter for all the transactions, the code is reset every day. It may be handled by the IVR application.
Authorization Number	I	N	6	0	64	69	It may be filled with 000000 for the Message Module API invocation. Core may respond with a numeric value of 6 positions

DESCRIPTION	I/O	TYPE	LENGTH	Decimals	From	To	Values/Constraints
Transaction Type	O	A	1		70	70	1 = Normal Transaction 2 = Forced Transaction 3 = Reversal Transaction
Reply Code	I	A	5		71	75	It may be filled with 00099 for the Message Module API invocation. Core mayrespond with a numeric value of 5 positions
Reply Code Description	I	A	75		76	150	It may be filled with 75 blanks for the Message Module API invocation. Core mayrespond with an alphanumeric value of 75 positions padded with blanks if necessary.
Filler	O	A	99		151	250	It may be filled with 99 blanks

[0052] As stated early, every transaction implements its own variable part depending on its nature and functionality.

[0053] The present invention allows the following transactions via the Fixed Part, Variable Part interface (i.e., the modified ISO 8583 interface):

Processing Code	Description	Type	Acquiring Chanel	Switch
330000	Balance Inquiry (Account Number)	Non Monetary	IVR	2021
330000	Balance Inquiry (Account Number)	Non Monetary	WEB	2023
330000	Balance Inquiry (Account Number)	Non Monetary	MB	2026
311000	Balance Inquiry (ID Number)	Non Monetary	WEB	2023
311000	Balance Inquiry (ID Number)	Non Monetary	MB	2026

Processing Code	Description	Type	Acquiring Chanel	Switch
330000	Balance Inquiry (Account Number)	Non Monetary	SMS	2028
321000	Last Monetary Movement Inquiry	Non Monetary	IVR	2021
321000	Last Monetary Movement Inquiry	Non Monetary	SMS	2028
321000	Last Monetary Movement Inquiry	Non Monetary	WEB	2023
330000	Balance Inquiry (Account Number)	Non Monetary	Corporate WEB	2024
330000	Balance Inquiry (ID Number)	Non Monetary	Corporate WEB	2024
321000	Last Monetary Movement Inquiry	Non Monetary	MB	2026
321000	Last Monetary Movement Inquiry	Non Monetary	Corporate WEB	2024
401030	Third Party Transfers	Monetary	IVR	2021
401030	Third Party Transfers	Monetary	WEB	2023
401030	Third Party Transfers	Monetary	MB	2026
500002	Session Start	Non Monetary	Corporate WEB	2024
500002	Session Start	Non Monetary	WEB	2023
500002	Session Start	Non Monetary	MB	2026
500003	Access PIN Change	Non Monetary	Corporate WEB	2024
500003	Access PIN Change	Non Monetary	WEB	2023
500003	Access PIN Change	Non Monetary	MB	2026
500006	Access PIN recovery(Reset Indicator)	Non Monetary	WEB	2023
500006	Access PIN recovery(Reset Indicator)	Non Monetary	Corporate WEB	2024
500001	Access PIN recovery(PIN setting)	Non Monetary	Corporate WEB	2024

Processing Code	Description	Type	Acquiring Chanel	Switch
500001	Access PIN recovery(PIN setting)	Non Monetary	WEB	2023
500007	Access PIN recovery(Reset Indicator)	Non Monetary	WEB	2023
500007	Access PIN recovery(Reset Indicator)	Non Monetary	Corporate WEB	2024
330000	Balance Inquiry # Account/Cellphone	Non Monetary	POS	2014
340000	Balance Inquiry # Account/Cellphone	Non Monetary	POS	2014
001000	Goods and Services Buy (Card)	Monetary	POS	2014
061001	Goods and Services buy (Cellphone)	Monetary	POS	2014
261001	Goods and Services buy (Cellphone) void	Monetary	POS	2014
061002	IVR PIN Verification Goods and Services Buy	Monetary	POS	2014
261002	IVR PIN Verification Goods and Services Buy Void	Monetary	POS	2014
201000	Goods and Services Buy Void	Monetary	POS	2014
021000	Account Recharge	Monetary	POS	2014
221000	Account Recharge Void	Monetary	POS	2014
031000	Redemption	Monetary	POS	2014
231000	Redemption Void	Monetary	POS	2014

Cell Bank Software Application

Functionality

[0054] The Cell Bank or Mobile Bank Application of the present invention allows NBFI or bank customers to complete common banking transactions (for example, balance inquiries, transfers) using a mobile telephone. It allows NBFI or bank customers to manage their banking accounts from any location where there is access to a mobile telephone signal or Internet connection.

[0055] The Cell Bank application of the present invention may be based on a J2ME Midlet. The J2ME Midlet enables NBFI or bank customers and the NBFI or bank to communicate on a data network using the data network operator's wireless telephone connection. The Cell Bank

application of the present invention communicates with a mobile banking gateway to authorize a customer to use the application. The mobile banking gateway validates a user session and processes input and output messages to and from the Cell Bank Application. It is also responsible for communicating with the FEP to send the modified ISO 8583 messages of transactions generated.

Application Architecture

[0056] The Cell Bank Application of the present invention may provide a series of integrated applications configured to run on a client-server scheme. In one embodiment, the client application resides on a user's mobile telephone and acquires and manages data that may be necessary for a transaction on the NBFi Electronic Payment System (EPS) network of low-value transactions or a Bank FEP using ISO 8583 conversion when assembling transactions or communications to the account. The client application uses the communication capabilities provided by the mobile telephone to initiate a data connection with intermediate servers that act as middleware between the client and the NBFi or bank.

[0057] The connectivity architecture is based on the defining characteristic of contemporary mobile telephones, that is, the ability to access the Internet through the cellular network and transfer data via the HTTP protocol. The disclosed communication architecture capitalizes on Internet accessibility, data transfer via the HTTP protocol, and the increasing computing/processing power of mobile telephones, to reduce the amount of data exchanged over the technology platforms relied upon by the Cell Bank Application.

[0058] The Cell Bank Application of the present invention may reside on the customer's mobile telephone. The application may acquire data necessary to initiate a transaction from the network of low-value transactions. That data may be translated into and sent as ciphered messages converted to XML code. The XML code may include the data for initiating a transaction and may be delivered by middleware to the server through HTTP POST. The middleware translates the forwarded data into the proper information exchange format using the modified ISO8583 of the present invention.

[0059] The XML code used to initiate a requested transaction utilizes one or more tags that may be defined in terms of the parameters needed to be included for each transaction based on the modified ISO8583 standard used in connection with the financial network of low value transactions. Additionally, to meet basic security requirements, a cryptography program may be used to secure sensitive information related to the operations of the financial system of the present invention. The cryptography program may provide lightweight yet robust protections based on encryption of sensitive information as specified, for example, in W3C: XML Encryption Syntax and Processing.

[0060] It is important to note that, preferably, only certain information is encrypted because of the high computational/processing requirements of encrypting and decrypting large amounts of data in a reasonable time. Such encryption and message conversion operates in a temporary key made as a variable division polynomial generated by the FEP session, making each transaction unique and different from the next. Accordingly, it is generally preferable to only encrypt sensitive data such as PINs, account numbers, etc. But in this case such encryption generates less data and provides unique resolution at each end. This improves system performance while adding the value of added security. The middleware server may be used to implement the API 141, for example. The middleware server may also have access to a sessions database and write information in that database to keep track of communication sessions between users and the core server. The middleware server may also have access to database which may contain information to assist with the verification or validation of user accounts, for example. The middleware server may connect to a security database which may contain information that may be used to validate PINs.

Flow of Transaction Referrals

[0061] One feature of the Cell Bank Application of the present invention is that it allows a customer to initiate a purchase transaction at a point of sale by providing the seller only the customer's telephone number and a PIN, for example.

[0062] Taking into account the variables that come into play in this process, the transaction is classified by the point of sale device as "Card Not Present." This designation makes a transaction of special care due to potential fraud exposure for impersonating the actual user, and for business concerns, transactions classified as "Card Not Present" are subsequently customer verified. The verification process may require that the customer be contacted by telephone, whereby the customer is prompted to confirm or reject the transaction by providing a PIN code required for monetary transactions.

[0063] As each transaction is atomic, this transaction, which is hereafter defined as a "Referral" point of sale transaction may divide into two independent steps in accordance with the present invention. In accordance with one embodiment of the present invention, the first step, a point of sale transaction is pre-authorized and is maintained on the switch as pending verification. In the second step, the point of sale transaction is the customer's self-verification. Thus the second step is used to verify the first step. Upon execution of both steps, the "Referral" point of sale transaction is complete.

[0064] A modified form of the "Referral" transaction is the "Passive Hold" transaction. The "Passive Hold" transaction is also executed using the NBF's or bank's network of low value transaction. In accordance with the one embodiment of the present invention, the "Passive Hold" transaction is similar to the "Referral" transaction in all respects except that the seller at the point of sale is only made aware of the existence of the transaction at the time of the transaction.

[0065] FIG. 9 illustrates a process that involves several individual transactions, in whole, properly synchronized, which are referenced to as “Referrals.”

[0066] Fig. 9 illustrates three devices or modules involved in the processing of transactions involving referrals, the POS 1401, the terminal administrator module 1403, and an IVR interface 1405, which may reside in the authorization module 139 (Fig. 1). For simplicity, the Fig. does not show the process of converting the messages from modified ISO 8583 to standard ISO 8583.

[0067] In one embodiment the transaction flow is as follows:

[0068] 1. A customer initiates a purchase transaction using a mobile telephone number (no need for a plastic debit or credit card) by providing all required data for the transaction, including, for example, the customer’s mobile telephone number 1407. The POS builds a message with the internally programmed Merchant ID information and a series of standard characters including transaction’s parameters such as date, hour, amount and ancillary security encryption codes built for PCI Compliance for other type of transactions. The message also includes a specific code that is recognized by the FEP as a “Referral” transaction. That code is part of the transaction ID and is passed along the authorization process. The message is sent to the FEP (1451), for example, to the terminal administrator module (1403). The terminal administrator module verifies the amount of the transaction (1409) and identifies the transaction as a Referral transaction (1411). By identifying the transaction as a Referral, the system knows that completion of the overall transaction is dependent upon PIN verification over the IVR (1405). After completion of the process a temporary code is rendered. Such code is used to complete the set of all necessary parameters in the transaction at the POS described in next paragraph.

[0069] 2. The mobile telephone then receives a request to confirm the transaction through the IVR system, which prompts the user to confirm the transaction with the security code (PIN1 from account activation). Upon receipt and verification of the PIN1 (1413), the IVR will communicate a onetime security code for the user to provide to the merchant. To generate a onetime use security code, the terminal administrator receiving the PIN information (1419) from the IVR verifies the life of the referral 1421, verifies PIN information 1423, and pre-authorizes the transaction 1425. Upon pre-authorization a pre-authorization code is generated and part of this code may be used as the onetime use security code (PIN2).

[0070] 3. The seller at the point of sale is sent a message 1453 referencing the pending transaction 1415 along with a standby signal 1417, which can be displayed on a monitor or screen at the POS. This message is sent by the FEP in response to the Referral transaction request. The standby signal can include a friendly message such as "Processing Please wait." By the time the standby signal is received by the seller at the point of sale, the data necessary to initiate the second step 1455 of the transaction has been sent for confirmation by the FEP. This second step may be initiated if there is one of two events:

- The customer has previously successfully verified the PIN1 over the IVR, so that the customer

can advise the seller at the point of sale to press an approval key or softkey on the monitor that indicates "Passive Waiting," for example. Pressing the "Passive Waiting" softkey may be the trigger for the seller at the point of sale to communicate the transaction data verification response 1455 received as a result of the first "Referral" Transaction request.

- The predetermined wait time for "passive waiting" has lapsed, so the point of sale becomes unblocked by sending 1455 the response data received from the first "Referral" transaction request to determine whether the transaction can be verified.

4. At that point the verification of the PIN has been communicated by the user/customer through the mobile telephone regardless of the event occurring in the preceding step three. The terminal administrator is then prompted to verify whether the transaction was validated by the merchant with the PIN2 1427 (In one embodiment the IVR provides PIN2 to the customer and the customer in turn provides PIN2 to the merchant). This step involves the following alternatives:

- The FEP verifies that the merchant provided the correct PIN2 and the transaction is finally approved. The FEP then communicates to the seller 1431 at the point of sale that the transaction was approved and a receipt may be printed 1433.

- The FEP rejects the transaction because the merchant failed to provide a correct PIN2. The FEP then communicates 1431 to the seller at the point of sale that the transaction was rejected and a proper rejection receipt may be printed 1433.

The foregoing description of possible implementations consistent with the present invention does not represent a comprehensive list of all such implementations or all variations of the implementations described. The description of only some implementation should not be construed as an intent to exclude other implementations. For example, artisans will understand how to implement the invention in many other ways, using equivalents and alternatives that do not depart from the scope of the invention. Moreover, unless indicated to the contrary in the preceding description, none of the components described in the implementations are essential to the invention. It is thus intended that the specification and examples be considered as exemplary only, with a true scope and spirit of the invention being indicated by the following claims.

CLAIMS

What is Claimed is:

1. A system for processing electronic financial transactions comprising: at least one remote device for assembling data messages in a first format, the data messages including requests for authorization for conducting card-less financial transactions based on use of a mobile phone number as a reference to a user account (or a combination of access number, selection upon answering to multiple accounts or financial products linked to Telephone number); an application programming interface residing in a server for receiving and converting said data messages into a second format; an acquirer module that acquires and decoding instructions in the data messages having a second format; and a processing module for executing instructions acquired by the acquirer module to read or write information into a back end database; wherein the acquirer module further communicates with the remote device to inform the remote device whether the requested financial transaction has been approved.
2. The system of claim 1, wherein the acquirer module includes an authorization module or a transaction module.
3. The system of claim 2, wherein the remote device includes a point-of-sale device or an electronic cash register and the acquirer module includes a terminal administration module for processing requests from the point-of-sale device or the electronic cash register.
4. The system of claim 2, wherein the authorization module verifies: whether an account to be debited has enough balance to complete a requested transaction; whether a PIN entered at remote device matches a PIN stored in the backend database; or whether a number of allowances is met.
5. The system of claim 2, wherein the authorization module issues a temporary code to be used as a security token in conducting financial transactions.
6. The system of claim 5, wherein the temporary code comprises the last two digits of a session ID.
7. The system of claim 1, wherein the first format is ISO 8583 modified to include a fixed part and a variable part.

8. A method for processing electronic transactions comprising setting up a user account, the method comprising: receiving a cell phone number associated with a new user; triggering a call through an interactive voice response system to verify the identification of the user and ownership of the cell phone by that user; receiving through a point-of-sale a personal identification number from the new user; setting up a new user account; receiving, through the point-of-sale, an amount of deposit and the user cell phone number; generating a temporary code and communicating said code to the point-of-sale; receiving the temporary code through the point-of-sale; and funding user account.

9. The method of claim 8, further comprising transmitting a text message to the user for confirmation that the account has been set-up and funded.

10. A method for transferring cash from a first user account to a second user account, the method comprising: receiving the cell phone number associated with the second user account, amount of transfer and personal identification number associated with first user account; validating the received cell phone number and second user account at a CMS; validating number of allowances of first user account at the CMS; receiving at an application programming interface a request for transfer in a first format; converting the request to a second format and sending the converted message to an authorization module; creating at the authorization module a temporary code if first user has sufficient funds; and writing credit to second user account.

11. The method of claim 10, further comprising: transmitting a text message to the first user for confirmation that transfer is complete.

12. A method for withdrawing cash from an automated teller machine comprising:

receiving a request in a first format by account holder for withdrawing cash from the teller machine; receiving a cell phone number from the account holder; verifying at a front end processing module whether request is accepted or declined based on cell phone number and available funds in holder account; transmitting temporary code to the account holder; receiving from teller machine a request in a first format that includes the temporary code, cell phone number of account holder, and user identification code; transmitting to financial institution server a request in a second format to dispense cash; and receiving authorization from said server to withdraw cash.

13. The method of claim 12, wherein said first format is a modified ISO 8583 message with a fixed part and a variable part and said second format is an ISO 8583 message.

14. The method of claim 12, further comprising transmitting a text message to the account holder to confirm cash dispensing transaction.

15. A method for electronic processing of purchases at a point-of-sale comprising: receiving, at an application programming interface, a message in a first format from a point-of-sale that includes a user cell phone number and a purchase amount; converting said message in the first format into a message in a second format; at the front end processing module, receiving said message in a second format and finding parameters within said message in a second format; initiating a voice interface routine at a voice interface module; placing a call to the user using the voice interface routine and obtaining user authorization for purchase transaction once user enters personal identification number; transmitting a temporary code to the point-of-sale; receiving, at an application programming interface, a second message in a first format from the point-of-sale including a renewed request for the purchase transaction, the renewed request including the temporary code; and authorizing the purchase transaction.

16. The method of claim 15, wherein said first format is a modified ISO 8583 message with a fixed part and a variable part and said second format is an ISO 8583 message.

17. A method for electronic processing of payroll disbursements comprising: receiving employer authorization for payroll pay with one or two security tokens; verifying that employer account is active and that employer has not exceeded number of allowances; receiving payroll pay request in a first format; converting the request into a second format; authorizing payroll pay if employer account has sufficient balance and number of allowances is not exceeded; and writing credit to employee accounts.

18. The method of claim 17, wherein said first format is a modified ISO 8583 message with a fixed part and a variable part and said second format is an ISO 8583 message.

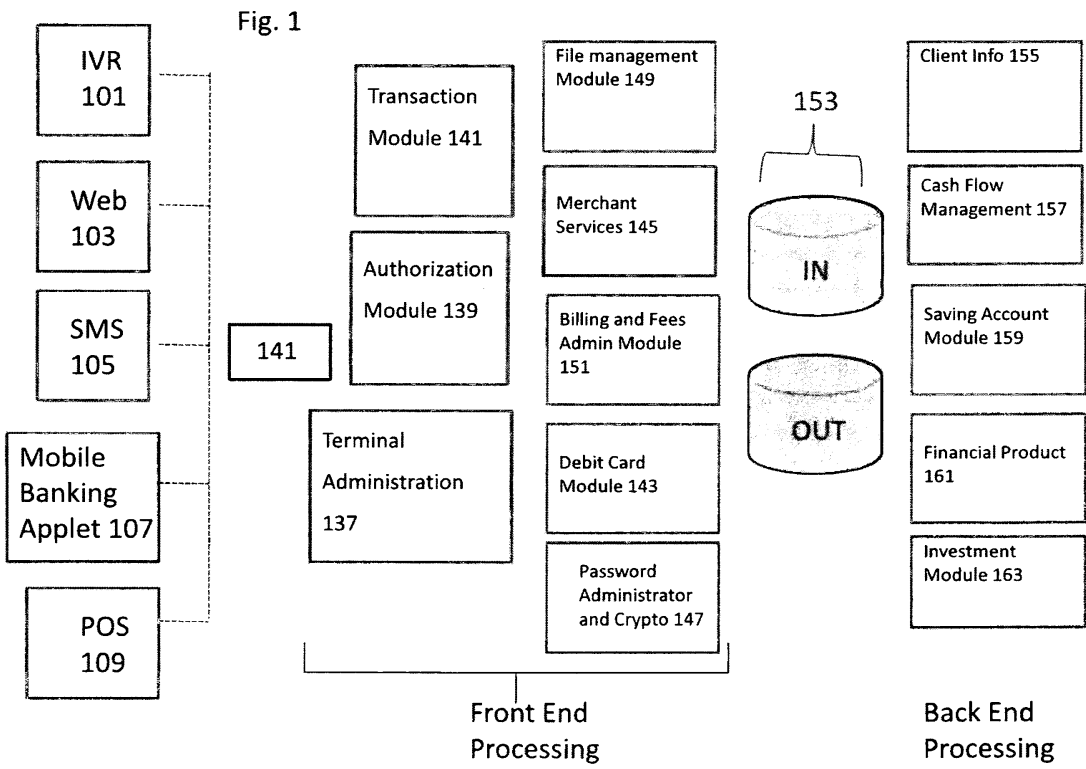
19. A method for electronic processing of payments to payees comprising: receiving a message from a cell phone in a first format that includes a request for payment to a payee, the message including a requestor's cell phone number, a requester's identification code, identification of a payee, and an amount of payment; converting the message into a second

format; authorizing payment if the requestor's account has sufficient balance, a number of allowances is not exceeded, and the identification code is valid; and writing credit to payee account.

20. The method of claim 19, wherein said first format is a modified ISO 8583 message with a fixed part and a variable part and said second format is an ISO 8583 message.

ABSTRACT

[0071] Systems and method of the present invention include a comprehensive system architecture that enables access to Non-bank financial institutions (NFBIs) and banks through point-of-sale devices and mobile telephones, for example. The present invention involves use of a modified ISO 8583 standard to allow users to interface with a front end processing system directly from non-traditional devices. The present invention also allows mobile banking with the NBFI through use of an application residing in a user's mobile telephone, which allows the encapsulation of user information as XML, for example, and the transmission of those over http while complying with the ISO 8583 standard, and further allowing encryption of certain user data, without having to resort to access to mobile banking website. In one aspect of the invention, a POS application may run on top of PCI to enable users to make purchases using funds pre-deposited in an NBFI account.



85

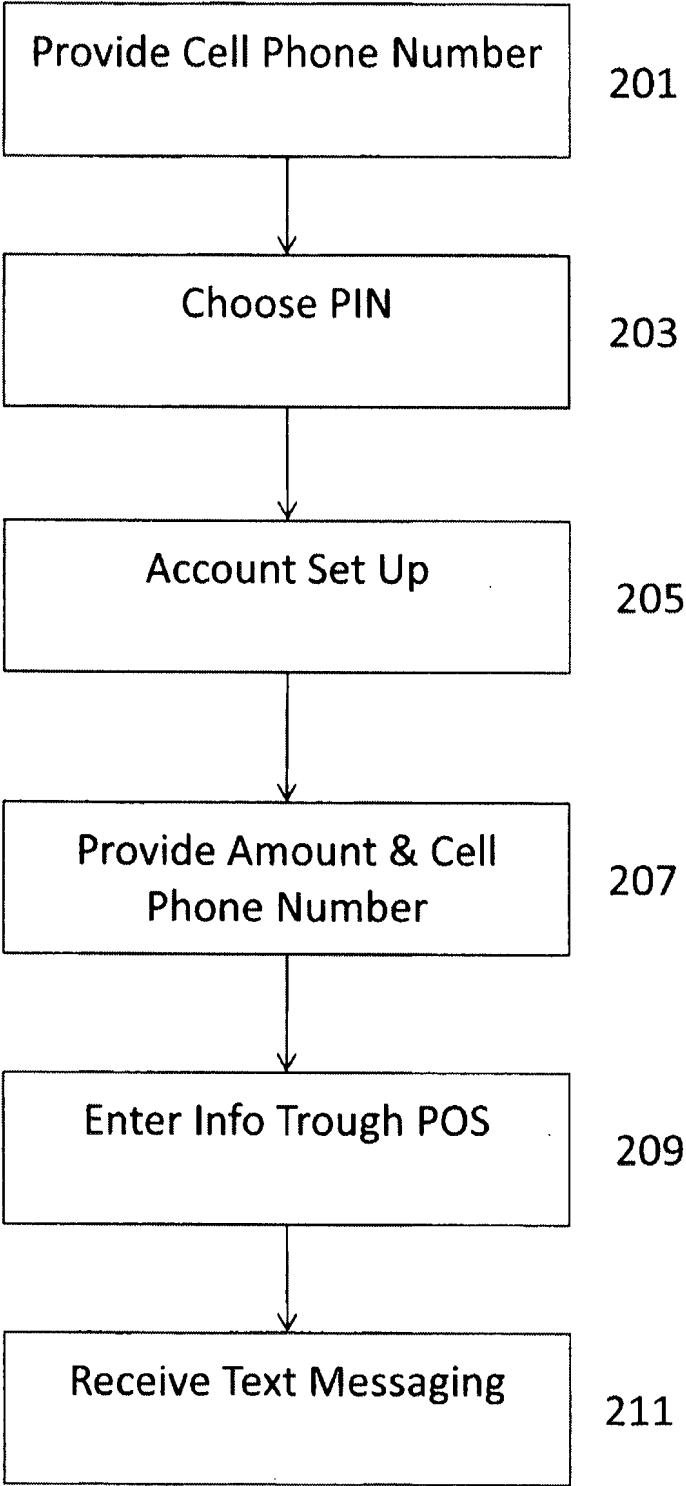


Fig. 2

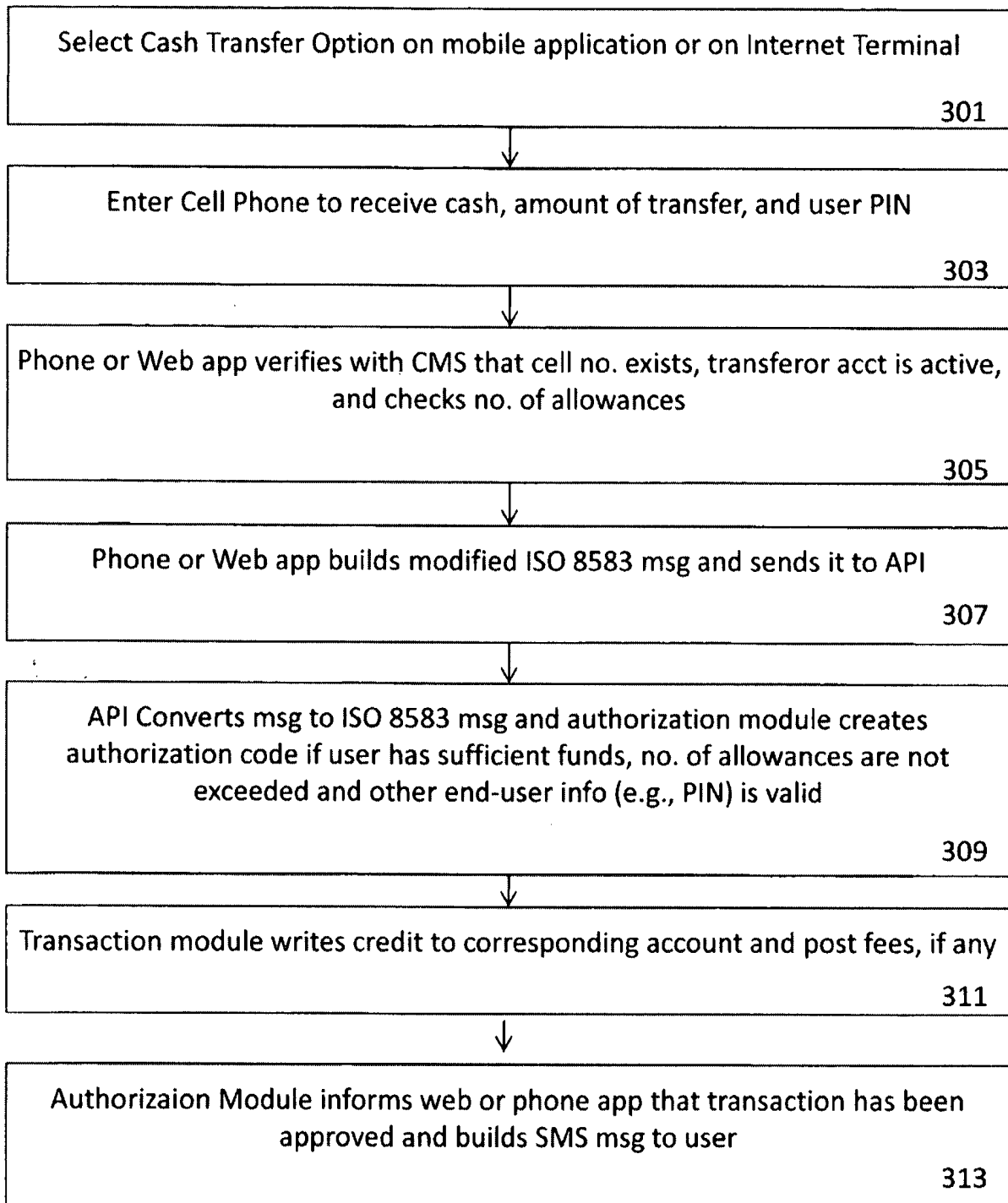


Fig. 3

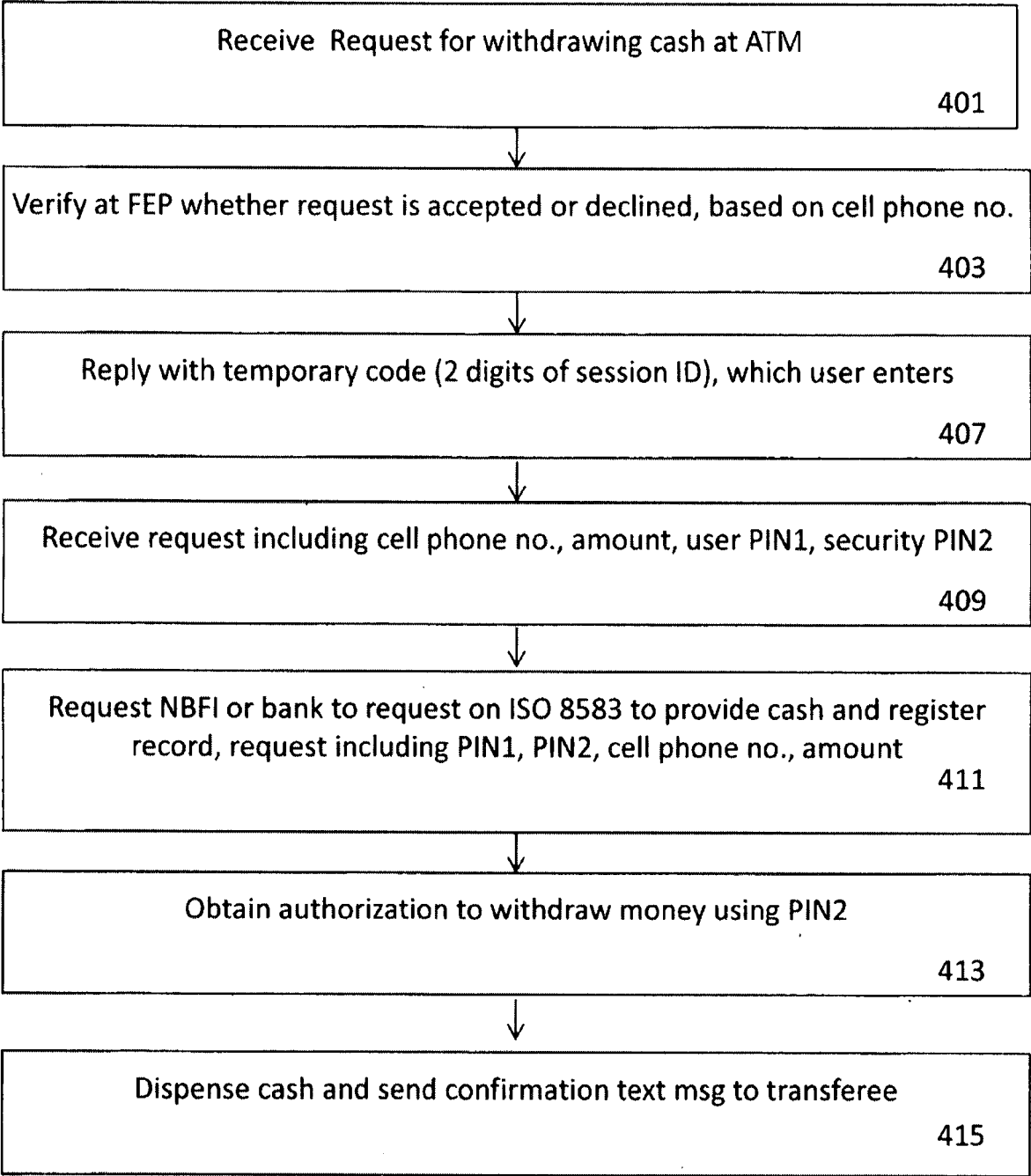


Fig. 4

28

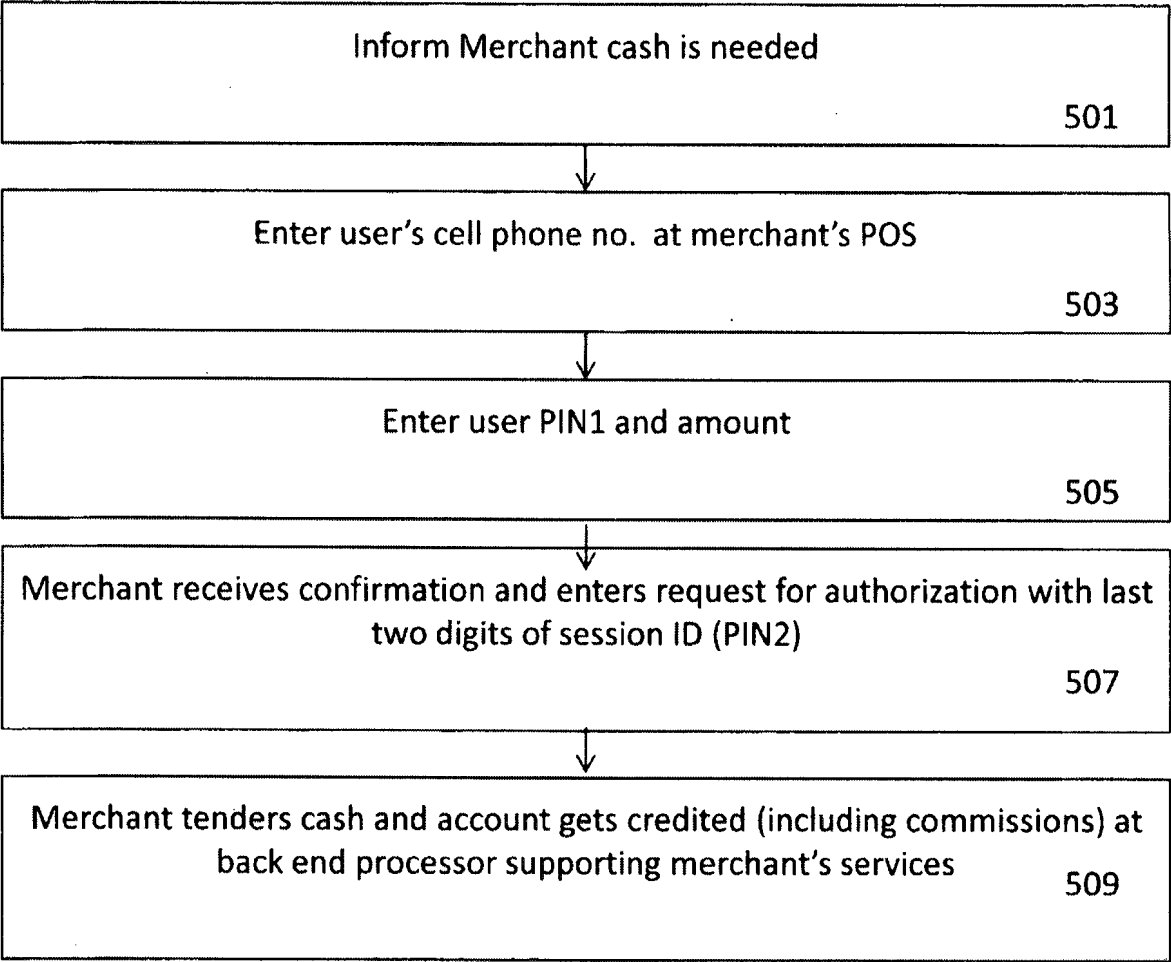


Fig. 5

Invention Title: SYSTEM AND METHOD FOR CONDUCTING FINANCIAL TRANSACTIONS

First Named Inventor: Federico L. Fuentes

Attorney Docket No: 1496.PLAT0002U

6/9

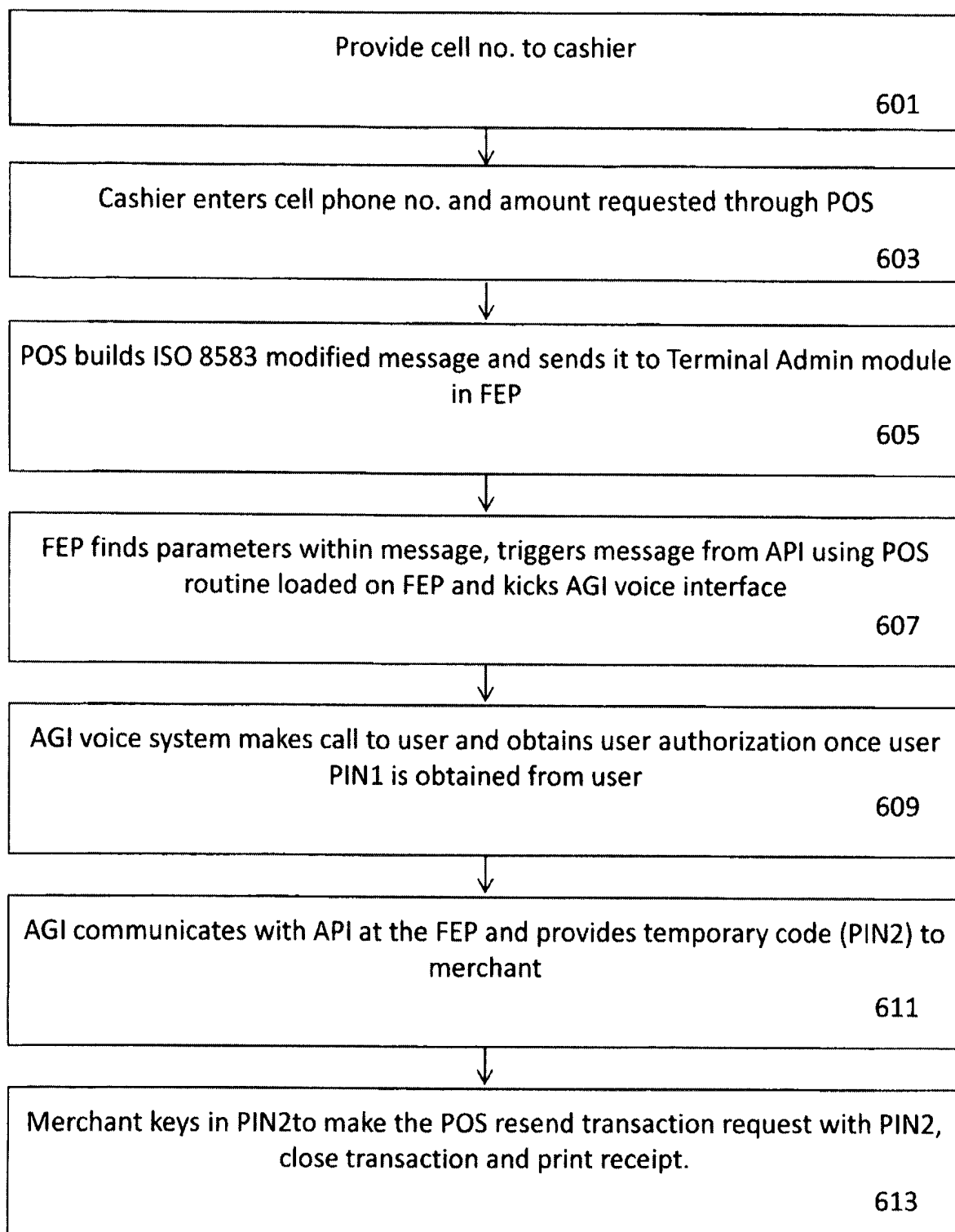


Fig. 6

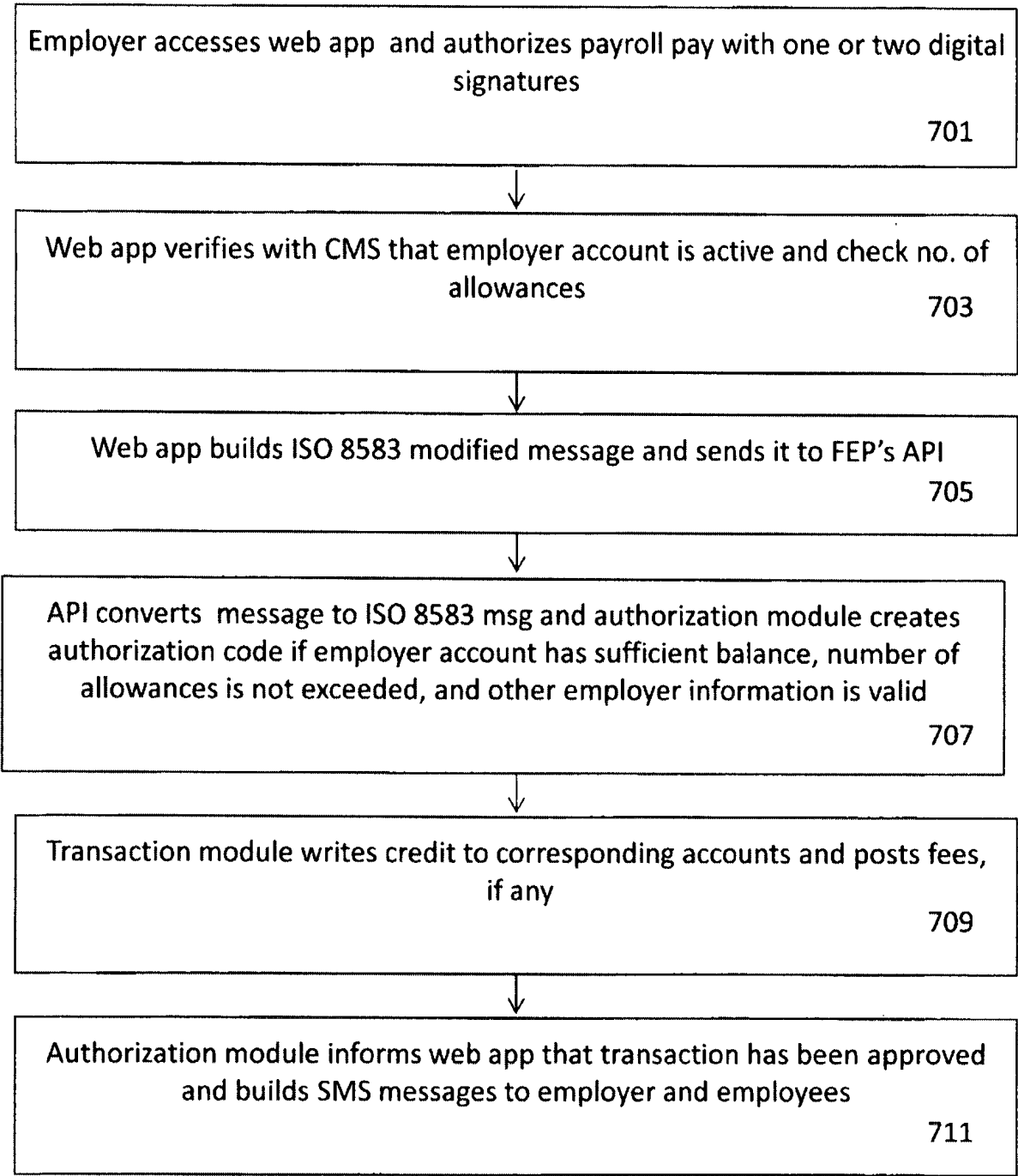


Fig. 7

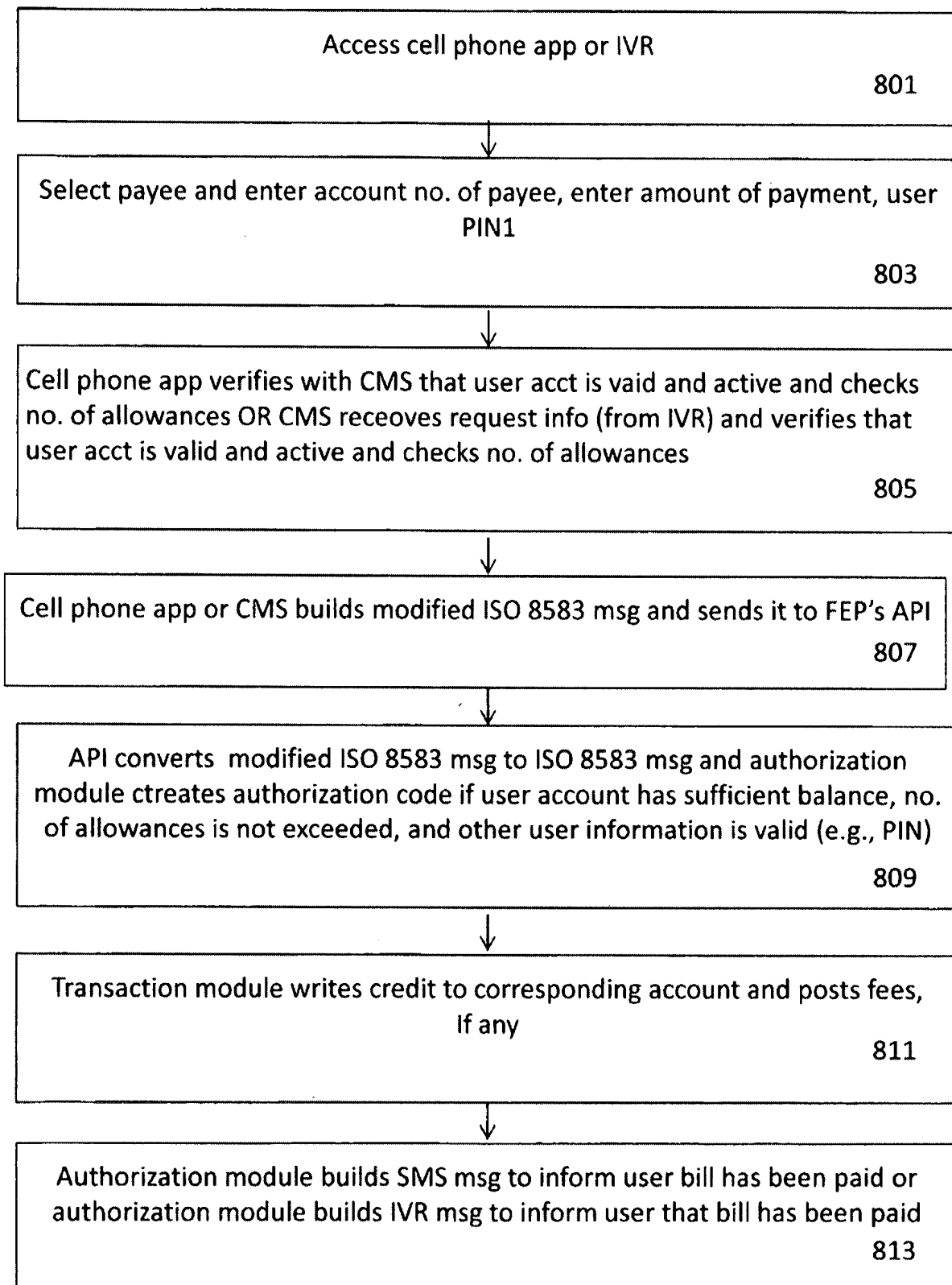


Fig. 8

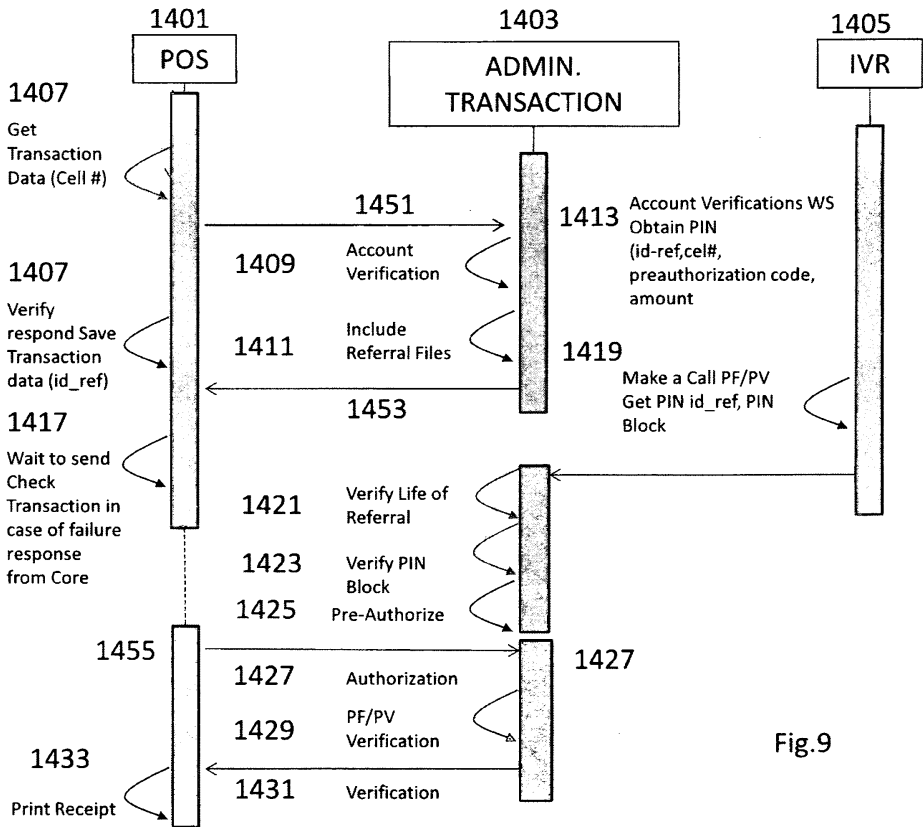


Fig.9



THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

June 20, 2012

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: 13/217,634

FILING DATE: August 25, 2011

THE COUNTRY CODE AND NUMBER OF YOUR PRIORITY APPLICATION, TO BE USED FOR FILING ABROAD UNDER THE PARIS CONVENTION, IS US13/217,634

**By Authority of the
Under Secretary of Commerce for Intellectual Property
and Director of the United States Patent and Trademark Office**



T. LAWRENCE

Certifying Officer

 Industria y Comercio SUPERINTENDENCIA		PLANILLA DE RADICACIÓN - DIGITALIZACIÓN DIARIA RELACIÓN DE ANEXOS	
Dependencia:		Fecha:	Recorrido:
Tipo de Radicación:		Entrada:	Salida:
		Traslado:	Convenio:
Radicador:			Planilla:
ID	No. Radicación	Cons	Item
1			1
2	12-121806-0		2
3			3
4			4
5			5
6			6
7			7
8			8
9			9
10			10
11			11
12			12
13			13
14			
15			
16			
17			
18			
19			
20			

Item	Unidad de Conservación
1	CD
2	Disquetes
3	DVD
4	Fotos
5	Libro
6	Muestra Física
7	Otros
8	Planos
9	Periódico
10	Publicación Periódica
11	Sobre blanco tamaño carta
12	Sobre blanco tamaño oficio
13	Sobre de manila

Observaciones
Folio 95 CD

ESTADOS UNIDOS DE AMERICA
A QUIEN PUEDA INTERESAR
Oficina de Marcas y Patentes de los Estados Unidos

Junio 20 de 2012

LA PRESENTE ES PARA CERTIFICAR QUE LO ANEXO ES COPIA FIEL DE LOS REGISTROS DE LA OFICINA DE MARCAS Y PATENTES DE LOS ESTADOS UNIDOS DE AQUELLOS DOCUMENTOS QUE A CONTINUACION IDENTIFICAN LA SOLICITUD DE PATENTE QUE CUMPLIO CON LOS REQUISITOS PARA QUE LE FUERA OTORGADA UNA FECHA DE PRESENTACION BAJO EL 35 USC 111.

NUMERO DE SOLICITUD: 13/217,634

FECHA DE PRESENTACION: AGOSTO 25, 2011

EL CODIGO DE PAIS Y NUMERO DE SU SOLICITUD DE PRIORIDAD, QUE SERÁ UTILIZADO PARA PRESENTACIÓN EN EL EXTRANJERO BAJO LA CONVENCION DE PARIS, ES *US13/217,634*

Por la autoridad del

Subsecretario de Comercio para Propiedad Intelectual y Director de la Oficina de Marcas y Patentes de los Estados Unidos



T. LAWRENCE

Oficial que Certifica

SISTEMA Y METODO PARA LA REALIZACION DE TRANSACCIONES FINANCIERAS

CAMPO DE LA INVENCION

[0001] La presente invención está relacionada con los sistemas de procesamiento de datos y métodos para la realización de transacciones financieras en una red. En particular, la presente invención se refiere a los sistemas y métodos integrados que suministran un acceso seguro a capital y que permiten transacciones financieras por medio del uso de tecnología inalámbrica, tal como dispositivos móviles.

ANTECEDENTES DE LA INVENCION

[0002] Los negocios dedicados al cambio de cheques y pago de facturas en nombre de otros se esmeran en los Estados Unidos así como en otras partes del mundo. Las familias de bajos ingresos están prácticamente forzadas a utilizar estos servicios debido a los altos honorarios cobrados por los bancos por mantener un saldo bajo en una cuenta y debido a los requisitos de altos depósitos iniciales para abrir una cuenta. Los trabajadores migrantes también se ven obligados a utilizar estos servicios puesto que los bancos no permiten a una persona abrir una cuenta sin que suministre una dirección en los Estados Unidos. En general, un gran porcentaje de la población en los Estados Unidos no tiene acceso a capital o servicios financieros a través de los bancos. Esto es algo que las compañías de cambio de cheques aprovechan al hacer préstamos de corto plazo a un interés muy alto. Estas condiciones han creado un problema que esencialmente, pone en peligro la seguridad de las personas que siempre llevan dinero en efectivo. Estas condiciones también crean un problema potencial ya que pueden afectar la capacidad de una autoridad fiscal para recaudar los impuestos sobre transacciones que no pueden ser rastreadas.

[0003] Las instituciones financieras no bancarias ("NBFIs" – por sus siglas en inglés) se han convertido en una alternativa eficiente para los bancos en términos de suministrar servicios financieros a personas con un patrimonio o recursos económicos limitados. El servicio de aceptación de depósitos monetarios del público está típicamente regulado o controlado por el estado o la ley y las regulaciones federales y estas NBFIs no están exentas de tales leyes o reglamentos. A nivel global, estas NBFIs permiten un acceso más amplio a los

servicios financieros, especialmente a las personas que residen lejos de las grandes ciudades. De hecho, uno de los principales aspectos que limitan la facilidad de acceso a bancos alrededor del mundo es la escasez de sucursales que ofrecen servicios al cliente, etc. No sorprende que uno de los objetivos de las NBFIs sea incrementar el número de lugares donde los clientes pueden ser atendidos por medio del incremento en el número de canales no tradicionales, que autorizan a las instituciones bancarias a ofrecer servicios financieros a través de las NBFIs, tales como tiendas, supermercados, etc. Aunque, las NBFIs constituyen una herramienta contra la exclusión financiera, aún persiste una necesidad de un sistema que permita tener un acceso más fácil a capital o a los servicios financieros a través de las NBFIs y los bancos.

RESUMEN DE LA INVENCION

[0004] A continuación se presenta un resumen simplificado de la invención con el fin de suministrar un entendimiento básico de algunos aspectos de la invención. Este resumen no es una descripción amplia de la invención. No pretende identificar ni elementos clave ni críticos de la invención ni delimitar el alcance de la invención. Su único propósito es presentar algunos conceptos de la invención en una forma simplificada como un preludio a la descripción más detallada que será presentada más adelante.

[0005] La presente invención incluye una arquitectura de un sistema integral que permite el acceso a las NBFIs (o bancos) a través de, por ejemplo, dispositivos de punto de venta y de teléfonos móviles. En una incorporación de la presente invención, el estándar ISO 8583 ha sido ampliado con el fin de permitir a los usuarios una interfase con un sistema de procesamiento front end (que interactúa con los usuarios) directamente desde dispositivos no tradicionales.

[0006] En otra incorporación de la presente invención, la banca móvil con las NBFIs o los bancos puede ser lograda a través del uso de una aplicación que resida en el teléfono móvil de un usuario, que permita el encapsulamiento de la información del usuario como XML, por ejemplo, y la transmisión de aquellas sobre http mientras cumplan con la expansión del anteriormente mencionado ISO 8583, y además permita la encriptación de ciertos datos del usuario. En otra incorporación de la presente invención, una aplicación POS puede ser ejecutada

sobre el estándar PCI para permitir a los usuarios hacer compras utilizando fondos depositados previamente en una cuenta NBFÍ. Para lograr esto, la aplicación POS puede iniciar una sesión con la NBFÍ o el banco y utilizar un mensaje encriptado obtenido a través de tal primera sesión para encriptar información como parte de una segunda sesión que entonces será utilizada para finalizar la transacción mientras la primera sesión expira.

[0007] La siguiente descripción y los dibujos anexos establecen en detalle ciertos aspectos ilustrativos de la invención. Estos aspectos son indicativos, sin embargo, de solo unos pocos de los diversos modos en los cuales los principios de la invención pueden ser empleados y la presente invención está destinada a incluir la totalidad de tales aspectos y sus equivalentes. Otras ventajas y características novedosas de la invención se harán evidentes de la siguiente descripción detallada de la invención cuando sean consideradas en conjunto con los dibujos.

BREVE DESCRIPCION DE LOS DIBUJOS

[0008] La Fig. 1 ilustra una arquitectura de una transacción financiera de acuerdo con una incorporación de la presente invención;

[0009] La Fig. 2 ilustra un método para la creación de una cuenta de usuario de acuerdo con una incorporación de la presente invención;

[0010] La Fig. 3 ilustra un método para transferencia electrónica de efectivo a otra cuenta de acuerdo con una incorporación de la presente invención;

[0011] La Fig. 4 ilustra un método para obtener el uso de un PIN de uso por una sola vez para que sea utilizado en un ATM de acuerdo con una incorporación de la presente invención;

[0012] La Fig. 5 ilustra un método para el procesamiento electrónico de retiro de efectivo a través del uso de POS de acuerdo con una incorporación de la presente invención;

[0013] La Fig. 6 ilustra un método para procesamiento electrónico de compras en el sitio de un comerciante de acuerdo con una incorporación de la presente invención;

[0014] La Fig. 7 ilustra un método para procesamiento electrónico de desembolsos de nómina de acuerdo con una primera incorporación de la presente invención;

[0015] La Fig. 8 ilustra un método para procesamiento electrónico de pagos a beneficiarios de acuerdo con una segunda incorporación de la presente invención; y

[0016] La Fig. 9 ilustra un flujo de transacciones relacionadas con el procesamiento electrónico de compras o retiros de efectivo de acuerdo con una incorporación de la presente invención.

DESCRIPCION DETALLADA DE LAS INCORPORACIONES ILUSTRATIVAS

[0017] La presente invención de ahora en adelante será descrita de forma más completa con referencia a los dibujos que la acompañan, en la cual serán mostradas las incorporaciones preferidas de la invención. Esta invención puede, sin embargo, ser incorporada de muchas formas diferentes y no debiera ser interpretada de una forma limitada a las incorporaciones establecidas en la presente. Más bien, estas incorporaciones se suministran de forma tal que esta divulgación sea exhaustiva y completa, y transmita plenamente el alcance de la invención para los expertos en la técnica.

[0018] Como se podrá apreciar por aquellos expertos en la técnica, porciones de la presente invención pueden ser incorporadas como un método, sistema de procesamiento de datos, o un producto de programa de computador. En consecuencia, estas porciones de la presente invención pueden tomar la forma de una incorporación total de hardware, una incorporación total de software, o una incorporación que combine aspectos de software y hardware. Además, porciones de la presente invención pueden ser implementadas como un producto de programa de computador en un medio de almacenamiento utilizable de un computador que tiene un código de programa legible por computador en el medio. Cualquier medio legible por computador adecuado se puede utilizar incluyendo, pero no limitado a, dispositivos de almacenamiento estáticos y dinámicos, discos duros, dispositivos ópticos de almacenamiento, y dispositivos de almacenamiento magnético.

[0019] La presente invención está descrita a continuación con referencia a ilustraciones de métodos, sistemas, y productos de programa de computador de acuerdo con las incorporaciones de la invención. Se entenderá que los bloques de las ilustraciones, y combinaciones de bloques en las ilustraciones, pueden ser implementadas por instrucciones de programa de computador, dispositivos de hardware, o una combinación de ambos. Estas instrucciones de programa de computador pueden ser suministradas a un procesador de un computador de uso general, computador de uso específico, u otro dispositivo de procesamiento de datos programable para producir una máquina en particular, de tal manera que las instrucciones, que se ejecutan a través del procesador del computador u otro dispositivo programable de procesamiento de datos, implemente las funciones especificadas en el bloque o los bloques.

Transacciones Implementadas Mediante ISO 8583 Modificado

[0020] La Fig. 1 ilustra una arquitectura que ejemplifica el sistema de la presente invención de acuerdo con una incorporación. El sistema incluye un número de módulos de procesamiento front end en interfase con dispositivos remotos a través de una interfase de mensajes ISO 8583, 141 modificada de acuerdo con la presente invención. Aunque el ISO 8583 define un estándar común, no es típicamente utilizada por sistemas o redes transaccionales financieras. En cambio, cada red adapta el estándar para su propio uso con campos personalizados y usos personalizados.

[0021] La colocación de los campos en diferentes versiones del estándar varía. Por ejemplo, los elementos de moneda de las versiones de 1987 y 1993 del estándar ISO 8583 ya no se utilizan en la versión 2003, que tiene al tipo de moneda como un subelemento de cualquier elemento de importe financiero. Al momento de este escrito, la ISO 8583:2003 aún no ha logrado una amplia aceptación.

[0022] Un mensaje de ISO 8583 está compuesto por las siguientes partes:

Un indicador de tipo de mensaje (MTI)

Uno o más mapas de bits, que indican cuales elementos de datos están presentes

Elementos de datos, los campos del mensaje.

[0023] Los dispositivos o sistemas remotos que pueden acceder el sistema de la presente invención incluyen una caja registradora electrónica (ECR) (no se ilustra); Un módulo de Respuesta Interactiva de Voz (IVR) 101, un dispositivo de punto de venta (POS) 109, que puede comunicarse con un campo lector de comunicaciones cercano (NFC) para leer la información desde una tarjeta de crédito o dispositivo móvil, por ejemplo, un dispositivo de cómputo con acceso a Internet (Web) 103; un teléfono celular con una aplicación para banca móvil (MB) 107; y un dispositivo remoto capaz de recibir mensajes SMS (SMS) 105. Los dispositivos remotos 101, 103, 107, y 109, pueden comunicarse con la API (*Application Programming Interface*) 141 a través de Internet o los circuitos de la Red de Punto de Acceso (APN). Algunos de estos son dispositivos remotos "smart" (inteligentes) que pueden ensamblar un mensaje modificado ISO 8583 y enviarlo a la API 141. Para otros dispositivos con capacidades limitadas, un servicio de administración de clientes (CMS) (no se ilustra) puede ser utilizado para ensamblar un mensaje modificado ISO 8583 y enviar el mensaje modificado correspondiente ISO 8583 a la API 141. Por ejemplo, El CMS verifica la información recibida por los dispositivos antes de ensamblar el mensaje modificado ISO 8583. en general, el CMS verifica que un número telefónico celular particular exista, como en una incorporación de la presente invención el número telefónico celular de un usuario es utilizado como el número de cuenta, verifica que la cuenta del usuario esté activa, y verifica que el máximo número de autorizaciones (por ejemplo, el número de transacciones permitido por mes, día, etc.) no haya sido excedido. La información verificada y suministrada por el CMS puede ser utilizada para ensamblar mensajes modificados ISO 8583. El CMS entonces puede enviar el mensaje modificado ISO 8583 al AP 141 o este puede reenviar parámetros de verificación a un dispositivo inteligente para el ensamblar del mensaje modificado ISO 8583.

[0024] Como se mencionó, los dispositivos remotos pueden ser utilizados para el intercambio de mensajes modificados ISO 8583 con el API 141, que reside en un servidor de conmutación. Otros componentes del servidor de conmutación pueden incluir un modulo de conmutación, un módulo ATM, un módulo ACH, y un

módulo para utilizar en interfase con otras redes. Una de las funciones del API 141 es convertir los mensajes modificados ISO 8583 en mensajes estándar ISO 8583. Otra función incluye el paso de aquellos mensajes ISO 8583 a otros módulos que son parte del sistema de la presente invención, por ejemplo el módulo de administración del terminal 137 o el módulo de autorización 139. Cuando el API 141 conduce mensajes con esos módulos, por ejemplo, la transacción financiera se conoce como una transacción de circuito cerrado (closed loop transactions). Cuando el API 141 intercambia mensajes con un módulo de conmutación, el modulo ACH o los otros módulos de red en el servidor de conmutación, los mensajes desde el API 141 dejan la arquitectura de red ilustrada en la Fig. 1, y como tal, las transacciones que involucran tal tipo de mensajes se conocen como transacciones de circuito abierto (open loop transactions), como sería comprendido por una persona de conocimiento común en la técnica.

[0025] El sistema de la presente invención puede incluir módulos de procesamiento "front end" (FEP). En una incorporación de la presente invención, el FEP incluye módulos de adquiriente (es decir, los módulos 137-141 que adquieren instrucciones o comandos desde los dispositivos remotos) y módulos de procesamiento (es decir, módulos 143-151 que ejecutan instrucciones para leer o escribir información en la base de datos 153). El FEP puede ser implementado en un servidor separado del servidor de conmutación. En una incorporación de la presente invención, los módulos de adquisición y procesamiento pueden ser implementados como máquinas virtuales separadas que corren sobre el mismo servidor.

[0026] Los módulos de adquisición FEP pueden incluir un módulo de administración de terminal 137, un módulo de administración 139 y un módulo de transacción 141. El modulo de administración de terminal 137 se utiliza para procesar solicitudes desde los dispositivos POS y ECR. Estas solicitudes pueden incluir la identificación del POS o ECR, información del origen de la cuenta, información de la cuenta de destino, y suma de la transacción y de gastos de transacción.

[0027] En una incorporación, la transacción que solicita desde dispositivos remoto diferentes de un POS o ECR se puede pasar por el API 141 directamente

en el modulo de autorización 139. El modulo de autorización 139 verifica si la cuenta a ser debitada tiene saldo suficiente para completar la transacción, que el PIN ingresado para autenticación del usuario (por ejemplo, PIN1) concuerde con el PIN almacenado en la base de datos 153, y verifique que el número de autorización se cumpla. El PIN es internamente recreado por el modulo de contraseña y criptografía 147, el cual puede ser implementado como una tarjeta de criptografía con base en un hardware. Tras la autorización, el modulo 139 emite un código de autorización. En una incorporación, los dos últimos dígitos del código de autorización pueden ser utilizados como un código de uso temporal/ de una sola vez (es decir, PIN2) para realizar las transacciones por ATM o las transacciones de compras.

[0028] El código de autorización se pasa al modulo de transacción 141, que genera instrucciones para créditos o cuentas escritas, post débito a cuentas, así como honorarios. Por ejemplo, si la transacción solicitada es para una compra, el modulo de transacción 141 instruye al modulo de servicios mercantil 145 a inscribir un crédito en la cuenta del comerciante en la base de datos 153, instruye al módulo de tarjeta débito 143 para inscribir un débito en la cuenta del usuario en la base de datos 153, e instruye la facturación y al módulo de alimentación administrativa 151 para fijar unos honorarios asociados con la transacción. Como las transacciones han sido completadas, el modulo de administración de archivos 149 guarda un registro de las transacciones procesadas (por ejemplo, tiempo de transacción, etc.) 141.

[0029] En otro aspecto de la presente invención, la base de datos 153 es compartida por los módulos FEP y el procesamiento back end (parte que procesa la entrada) del (BEP). En la incorporación ilustrada, los módulos BEP incluyen el módulo de información de clientes 155, el módulo de manejo de flujo de caja 157, el módulo de cuentas de ahorro 159, el módulo de producto financiero 161, y el módulo de inversión 163. Estos módulos BEP están asociados con funciones tradicionales de banca. En una incorporación, éstos pueden ser implementados como módulos utilizados para crear reportes que contengan información básica del cliente (155), información acerca del manejo del flujo de caja de un cliente (157), información relacionada con los ahorros de un cliente (159), información acerca de productos financieros utilizados por un cliente (161), e información acerca de las inversiones de un cliente (163).

[0030] Una de las ventajas de la presente invención es que los usuarios del sistema pueden activar o crear cuentas sin la necesidad de someterse a todas las formalidades impuestas bajo un modelo bancario tradicional. En consecuencia, algunas de las funciones bancarias más tradicionales asociadas con el procesamiento BEP puede que no sean necesarias para un usuario de la presente invención. Por ejemplo, en una incorporación preferida, un usuario puede ir a un almacén o tienda que opera un POS para abrir una cuenta con una NBFi o banco, o para abrir en una NBFi o banco una cuenta débito prepagada que tenga un límite en términos de número de transacciones y límite de efectivo así como los medios para informar acerca del lavado de dinero a las autoridades. El sistema aun permite que estas transacciones tengan lugar en el sitio. La presente invención no inhibe el proceso KYC (Know Your Client – Conozca a su Cliente) si es obligatorio y el BEP permite el procesamiento de transacciones que involucran contacto cara a cara para la creación de cuentas o el proceso simplificado de creación de cuentas de la incorporación preferida de la presente invención. El usuario o cliente nuevo le entregaría dinero en efectivo al comerciante para depositar en una cuenta asociada con el número telefónico del móvil de tal cliente. Utilizando la interfase IVR 101, un cliente de una NBFi o banco que implemente el sistema de la presente invención puede marcar en el sistema para encontrar información de saldos, Transacciones autorizadas, etc. Utilizando la interfase de red, un usuario del sistema, por ejemplo un empleador, puede iniciar sesión en el sistema y autorizar los pagos de nómina mediante la transferencia de fondos de una NBFi o banco, por ejemplo, a la cuenta de un empleado. También, el sistema de la presente invención puede enviar mensajes de texto (por ejemplo SMS) para confirmar que las transacciones han sido completadas. Estas transacciones ejemplificantes serán discutidas en detalle más adelante.

[0031] La Fig. 2 ilustra un tipo de transacción que puede ser ejecutada a través del uso de un POS en el cual un nuevo cliente de la NBFi o banco que utiliza la presente invención puede activar una cuenta en la ubicación de un comerciante. El comerciante es designado como Correponsal Independiente o tienda autorizada por el banco o la NBFi. Un cliente puede hacer un depósito inicial en una ubicación seleccionada, por ejemplo, en cualquiera de las tiendas asociadas o Corresponsales Independientes. En el paso 201 un comerciante podría ingresar en el POS 109, por ejemplo, el número celular asociado con el nuevo cliente. El

cliente podría esperar hasta que el sistema le llame para verificar la identificación del propietario del teléfono celular. El cliente entonces, podría escoger un PIN (paso 203) y este PIN es ingresado en la conexión POS al FEP para aprobar una autorización solicitada por el dispositivo POS, que forma parte del paso de configuración de la cuenta 205, para reiniciar el cumplimiento de la solicitud mediante la introducción de un código temporal suministrado al Comerciante por el sistema, que permite a la transacción seguir adelante con todos los parámetros incluidos habilitados por el intercambio de información entre el titular de la cuenta (vía Telefónica), El comerciante que suministra la facturación y permite el pago electrónico con confidencialidad de la información, y la validación y la decisión por el consumidor para completar el pago, y la notificación de la decisión con el código temporal al operador del POS del Comerciante. El POS entonces obtendrá los parámetros de confirmación y adicionales para verificar la validez y la información acerca del propietario de la cuenta. El sistema de la presente invención sería entonces configurar la cuenta en el paso 205. Tras la recepción del efectivo y tras los métodos de activación de cuenta por la NBFi o el Banco, el comerciante puede introducir el número del titular de la cuenta del teléfono celular en el POS 109 en los pasos 207 y 209 para abonar en la cuenta al recibir el efectivo para "acreditar" la cuenta. Luego de que la cuenta ha sido financiada (fondeada), el cliente recibe un mensaje de texto vía un Sistema de Mensaje Corto (SMS) la confirmación de la transacción en su teléfono celular a través de un mensaje SMS (en la parte superior de la cantidad anterior a debitar de su cuenta por (IVR), por ejemplo (paso 211).

[0032] La Fig. 3 ilustra un método para transferir dinero en efectivo de un titular de cuenta en una NBFi o banco a otra. En el paso 301 el usuario selecciona la opción de transferencia de efectivo en un menú presentado por el MB 109 o Web 107, por ejemplo luego de que el MB 109 o Web 107 reconoce una transferencia o cuenta en particular, el usuario entonces ingresa el número de teléfono celular asociado con el otro titular de cuenta (paso 303) o número de tarjeta débito en la cuenta de destino así como la cantidad a ser transferida y el PIN de autenticación del usuario (es decir, PIN 1). La aplicación instalada en la terminal Web 107 o teléfono celular MB 109 entonces se comunica con el CMS para obtener la verificación de que los números de celular existen (permitido por la señalización de la red y la base de datos en CMS con los números registrados y cuenta asociada), que las cuentas están activas y verifica el número total de permisos para quien

transfiere (paso 305). En el paso 307 la aplicación de teléfono o red construye un mensaje modificado ISO 8583 sobre la información suministrada por el CMS y la envía al API 141.

[0033] En el paso 309 el API 141 convierte el mensaje recibido de un ISO 8583 modificado a un ISO 8583 estándar y el módulo de autorización 139 emite un código de autorización si la cuenta del usuario tiene fondos suficientes, el número de autorizaciones no es excedido, y otra información de los usuarios finales, tal como el PIN, es validada. En el paso 311 el modulo de transacción 141 se comunica con el modulo de servicios del comerciante 145 y el modulo de tarjeta débito 143 y encarga a estos módulos colocar el débito y el crédito en la base de datos 153 con respecto a las cuentas involucradas en la transacción. El modulo de transacción también instruye al modulo 151 para calcular y fijar los honorarios asociados con la transacción, si los hay. En el paso 313 el modulo de autorización informa a la red o aplicación de teléfono que reside en la Web 107 o MB 109 que la transacción ha sido aprobada y también elabora un mensaje que es enviado al usuario a través de la interfase SMS 111. El cedente y el cesionario reciben una confirmación por mensaje de texto (por ejemplo, SMS) de la transferencia.

[0034] La Fig. 4 ilustra un método para recuperar efectivo desde una NBFÍ o ATM autorizado de un banco de acuerdo con una incorporación de la presente invención. Esta transacción es preparada por el Cliente (usuario final) por anticipado por una suma específica utilizando la funcionalidad IVR. En el paso 401 el sistema recibe una solicitud para retiro de efectivo en un ATM, por ejemplo un ATM franquiciado a la marca o permite a una Red de ATM con la no solicitud de tarjeta del presente sistema. Si la solicitud es efectuada en el ATM, la solicitud puede ser activada por una tecla de función o una tecla pulsada por el usuario para indicar que el usuario busca retirar efectivo sin utilizar una tarjeta de ATM. La solicitud debe ser acompañada por el número celular del usuario. Antes de enviar la solicitud al API 141, el ATM se comunica con la Base de Datos CMS para determinar si la cuenta del usuario es válida, etc. En el paso 403, el ATM envía la solicitud al modulo de autorización 139 en el FEP a través de una interfase ATM (Aplicación ATM HUB para cambio de la transacción a FEP utilizando el estándar de mensaje ISO8583) y el FEP determina si la solicitud es aceptada o declinada (de acuerdo con los parámetros establecidos por las solicitudes del usuario cuando preparó la solicitud de retiro del ATM a través del IVR), basado en si la

cuenta asociada con el número telefónico celular está activa como una primera verificación para aprobar/declinar antes de proceder. Si la solicitud no es aceptada, el sistema genera una respuesta con un mensaje negando la solicitud de retiro. Por ejemplo, el usuario puede recibir un mensaje de texto (o el ATM puede mostrar tal mensaje) que informa que la solicitud ha sido denegada. En el paso 407, si la solicitud es aceptada, el usuario puede recibir un mensaje de texto con un código de autorización temporal para ingresar (PIN2). En una incorporación, este código temporal puede ser los dos últimos dígitos de un código de autorización generado por el módulo de autorización 139 en respuesta a la solicitud original.

[0035] En el paso 409, el usuario puede ingresar el código temporal junto con un PIN de usuario (PIN1) y la suma a ser retirada. En el paso 411, el ATM requiere a la NBTI licenciada o al banco solicitar una autorización ISO8583 para suministrar efectivo. Mientras esta solicitud está basada en ISO8583, las comunicaciones entre el ATM y el FEP están basadas en el ISO8583 modificado de la presente invención. En el paso 413, el emisor (banco licenciado o NBTI) autoriza el retiro de efectivo basado en PIN2 así como en parámetros adicionales. En el paso 415, el ATM recibe y procesa información para autorizar la transacción, este dispensa el efectivo, y este mensaje SMS se envía al usuario confirmación de la transacción.

[0036] La Fig. 5 ilustra a un alto nivel un método para la recuperación de efectivo en una ubicación de comerciante, a manera de ejemplo. Un método más específico puede ser implementado mediante el uso de un método similar al método descrito con respecto a la Fig.4 excepto que el usuario de la interfase podría ser un POS en lugar de un ATM. En referencia a la Fig.5, en el paso 501 un usuario solicita al comerciante efectivo. En el paso 503 el comerciante ingresa el final - en el POS. En el paso 505 el comerciante ingresa el número de teléfono celular del usuario, la suma de los retiros, y el PIN1 en la aplicación POS. En el paso 507 el comerciante ingresa una solicitud para autorización con el PIN2 (dos últimos dígitos de la sesión ID a ser incluidos en una transacción POS para completar la solicitud modificada ISO8583 o completar la autorización) recibe texto con la confirmación de que se puede ofrecer efectivo al usuario, asumiendo que el usuario tiene fondos. En el paso 509 el comerciante ofrece efectivo y las cuentas

del comerciante se acreditan en el procesador back-end que da soporte a los servicios del comerciante.

[0037] La Fig.6 ilustra un método para comprar bienes en el local del comerciante. Luego de que el cajero haya obtenido el monto total adeudado para la venta de bienes, el usuario suministra un número de teléfono celular asociado con la NBFi o cuenta bancaria al cajero (paso 601). En el paso 603 el cajero ingresa, a través de un ECR (o un dispositivo POS), el número de teléfono celular y la suma debida en el sistema. En el paso 605, el ECR construye un mensaje modificado ISO8583 solicitando autorización y enviándola al Módulo de Administración de Terminal 137 en el FEP. En una incorporación, el mensaje modificado ISO 8583 es construido luego de una verificación de que ciertos datos de usuario son recibidos desde CMS, como se describió anteriormente. En el paso 607 el FEP encuentra los parámetros de parte variable en el mensaje, activa un mensaje desde el API 141 utilizando una rutina POS/ECR cargada en el FEP, e inicia la rutina de interfase de voz (AGI, que representa Asterisk Graphics Interface). El sistema de voz de AGI hace una llamada al usuario y obtiene autorización del usuario una vez ingresa su número PIN asociado con la cuenta (paso 609). En el paso 611 el AGI se comunica con el API en el FEP y suministra un código temporal para usuario. En una incorporación, el código temporal puede ser los dos últimos dígitos de un código de autorización emitido por el módulo de autorización 139. En el paso 613, las claves de comerciante en el código temporal suministrado por el usuario para forzar la ECR/POS a reestructurar el mensaje modificado ISO 8583, envía el mensaje al API 137, y cierra la transacción.

[0038] La Fig.7 ilustra un método que puede ser utilizado por un empleador para hacer los pagos de nómina a sus empleados. En el paso 701 el empleador se registra en su cuenta a través de una interfase de red y luego autoriza el desembolso de la nómina. Este pago puede ser una transferencia de NBFi o cuenta de banco a una o más NBFi o cuentas de banco. En el paso 703 una aplicación de red solicita que la Base de Datos CMS verifique que la cuenta del empleador está activa, por ejemplo, y que el número de autorizaciones asociadas con la cuenta del empleador no han sido excedidas. Tras la verificación, en el paso 705 la aplicación de red construye un mensaje modificado ISO8583 y comunica el mensaje a la API 141. En el paso 707, el API 141 convierte el mensaje en un mensaje estándar ISO8583, y el modulo de autorización 139 emite

un código de autorización si la cuenta del empleador tiene saldo suficiente, el número de autorizaciones no es excedido, y otra información del empleador es válida. En el paso 709 el modulo de transacción 141 instruye a los módulos de procesamiento correspondientes en el FEP para escribir los créditos y débitos a las cuentas del empleador y empleado, junto con los costos asociados. En el paso 711 el modulo de autorización informa a la aplicación de red que las transacciones han sido aprobadas y elabora mensajes SMS que son enviados a los empleados y el empleador para confirmar los desembolsos.

[0039] La Fig. 8 ilustra un método para hacer pagos a un beneficiario (por ejemplo, una empresa de servicios públicos). En el paso 801 un usuario accesa a una aplicación de teléfono celular o marca en un sistema IVR para banca móvil. En el paso 803 el usuario accesa a una lista de beneficiarios mostrada en el teléfono celular o comunicada al usuario a través de la interfase IVR. El usuario selecciona al beneficiario e ingresa la información de cuenta del beneficiario, la suma a pagar, y un PIN.

[0040] En el paso 805 la Base de Datos CMS verifica que la cuenta del usuario esté activa y válida y verifica que el número de autorizaciones no haya sido excedido. Si el usuario está accedendo el sistema a través de la interfase MB 107, la aplicación del teléfono celular envía la solicitud para verificación al CMS y no elabora un mensaje modificado ISO 8583 hasta que el CMS verifica la cuenta del usuario. Si el usuario está accedendo el sistema a través de la interfase IVR 101, el CMS recibe la solicitud para verificación pero no necesita responder a la interfase IVR 101.

[0041] En el paso 807, la aplicación del teléfono celular elabora el mensaje modificado ISO 8583 para solicitar la transacción de pago al sistema cuando el usuario solicita tal transacción a través del MB 107. Alternativamente, el CMS con un guión de programa se adecuó para la elaboración del mensaje modificado ISO 8583 cuando el usuario solicita la transacción a través del IVR 101. Luego, o el MB 107 o el CMS envían el mensaje modificado ISO 8583 al API 141.

[0042] En el paso 809 el API 141 convierte el mensaje modificado ISO 8583 en un mensaje estándar ISO 8583 y envía el mensaje convertido, junto con parámetros en la parte variable del mensaje modificado ISO 8583, al módulo de

autorización 139. El modulo de autorización 139 entonces emite un código de autorización si la cuenta del usuario tiene saldo suficiente, el número de autorizaciones no ha sido excedido, y otra información de usuario es válida (por ejemplo, el PIN). En el paso 811 el modulo de transacción 141 instruye a los correspondientes módulos de procesamiento en el FEP para inscribir un crédito y débito a las cuentas correspondientes, junto con los costos asociados. En el paso 813, el modulo de autorización 139 elabora un mensaje SMS para informar al usuario que la factura ha sido pagada. Alternativamente, el modulo de autorización 139 elabora un mensaje IVR para informar al usuario a través de la interfase IVR 101 que la factura ha sido pagada.

[0043] Como ha sido mencionado, estas transacciones tienen lugar sin que el usuario haga uso de internet como el o ella tendrían que ver con la banca móvil convencional. La interfase entre el usuario y el sistema está basada en una variante del ISO 8583 como se explicó anteriormente. El formateo del mensaje modificado ISO 8583 será explicado a continuación. Los mensajes intercambiados entre el servidor de interfaz con los usuarios y el FEP también están basados en el estándar ISO8583.

[0044] Todas las transacciones anteriores pueden ser medidas en una Base de Datos CMS Primaria y otros módulos para elaborar el mensaje utilizando una secuencia de comandos específicos relacionados con todas las interfases que usan una librería escrita XML para el uso particular, de acuerdo con una incorporación de la presente invención. Tal Base de Datos sirve para controlar la actividad del usuario (incluyendo fraccionamiento de transacciones para esconder lavado) y límites de exposición o uso abusivo por los clientes y puede ser considerada un mecanismo de prevención de fraude. Tal Base de Datos está conectada a componentes de voz, mensajería, registro en la red y registro en la banca móvil. Se mide la actividad global de las cuentas de usuario independientemente de la interfase seleccionada por el usuario. Por ejemplo, en el sistema de procesamiento de voz este permite el enrutamiento cuando un número de teléfono celular asociado a una cuenta existe y bloquea el uso cuando la cuenta está marcada por cualquier razón o esta ha sido desactivada o no existe. Tal flujo de llamadas e intercambio de información puede ser controlado por una secuencia de comandos que manejan la capacidad de conmutación de voz y todas las otras interfases que intercambian la información a través de mensajes via XML.

Formato ISO 8583 Modificado

[0045] Los servicios de la industria financiera incluyen el intercambio de mensajes electrónicos relacionados con transacciones financieras. Un esfuerzo internacional fue llevado a cabo por la Organización Internacional de Estándares (ISO – por sus siglas en inglés) con una meta principal de defender una estructura única de mensaje para ser utilizada por todas las instituciones financieras alrededor del mundo. La ISO 8583 es el nombre del estándar internacional para transacciones financieras con mensajes originados en una tarjeta. Este define específicamente una estructura única de datos para el intercambio de mensajes entre redes financieras heterogeneas. Específicamente, el estándar determina una interfase común por la cual mensajes originados por una tarjeta de transacción financiera pueden ser intercambiados. Este especifica estructura, formato y contenido, elementos y valores de datos. Una ventaja de la presente invención es que permite a los usuarios llevar a cabo transacciones financieras, por ejemplo, compras sin la necesidad de una tarjeta débito o crédito mediante la conversión de los mensajes ISO 8583 modificados para que la red financiera “vea” la transacción sin tarjeta como una transacción de crédito o débito en total cumplimiento de parámetros obligatorios.

[0046] Las estructuras de mensajes ISO8583 tienen una serie de campos donde los datos transaccionales relacionados son almacenados. Estos campos son referidos como Bitmaps. La combinación de bitmaps distintos es lo que hace a las transacciones financieras que puedan ser procesadas por una institución financiera.

[0047] El estándar ISO8583 es únicamente el boceto principal a seguir por una entidad financiera con el fin de implementar las unidades transaccionales. La especificación de la aplicación puede permanecer en un nivel privado. Los diseñadores de la aplicación tienen completa libertad de diseño, dentro de la restricción general de la ISO 8583, para que tales mensajes sean convertibles al formato de interfase ISO 8583 para que el intercambio internacional pueda llevarse a cabo. La idea es que los desarrolladores de la aplicación financiera sean libres para implementar lo que consideren necesario si y únicamente si sus interfases de mensajes pueden ser trasladadas a especificaciones ISO8583 con el fin de promover el intercambio internacional.

[0048] La presente invención aprovecha la flexibilidad de la ISO 8583 mediante la implementación de una interfase común de mensajes enfocada en los datos para ser intercambiados en lugar de la complejidad de los esquemas en el mensaje de designación y declaración de esquemas de bitmap ISO 8583 en el mensaje. Esta característica se conoce aquí como la Parte Fija, Marcos de Mensajería de la Parte Variable, interfase. Uno de los beneficios de esta interfase ISO 8583 modificada es la facilidad de comunicación transaccional entre aplicaciones financieras de terceros y los procesadores back end convencionales que requieren conversión al estándar ISO8583.

Estructura de Datos de Parte Fija Parte Variable

[0049] En una incorporación de la presente invención, el intercambio de datos entre los módulos front-end y las aplicaciones de usuario final utilizados para interfase con la NBFi o el banco están basados en el uso de las Estructuras de Datos de Parte Fija Parte Variable. De acuerdo con esto, los datos para transacciones son puestos juntos en marcos específicos donde cada dato tiene una posición específica en el marco.

[0050] Los Marcos de Parte Fija / Parte Variable están basados en las premisas de la ISO 8583. La primera sección de un marco de comunicación a partir de esta implementación se denomina Parte Fija en el presente y contiene toda la información compartida que pertenece a todas las transacciones en el sistema, por ejemplo, el momento cuando las transacciones fueron ejecutadas, el código de transacción, el código de respuesta, y otros. La segunda sección del marco se denomina en el presente como la Parte Variable y permite enviar datos específicos dependiendo de la transacción que será ejecutada. Por ejemplo, si la operación que será ejecutada es Saldo de la Cuenta, entonces en la Parte Variable del mensaje ISO 8585 modificado, será enviado un mensaje con información básica del usuario. La sección de Parte Variable también permite establecer comunicación con terminales bancarias no tradicionales tales como teléfonos móviles y dispositivos POS. En una incorporación, el marco de Parte Fija, incluye 250 caracteres mientras que la Parte Variable es variable en su longitud.

[0051] La estructura de la parte Fija puede definirse como sigue:

DESCRIPCION	I/O	TIPO	LONGIT.	Decimal es	Des de	Hasta	Valores/Restricciones
Código de Aplicación	O	A	2		1	2	Valor Fijo = CS : Indica a FEP una transacción desde NBFU OPERADOR BANCARIO LICENCIADO
Código de Transacción	O	A	6		3	8	Indicador Alfanumérico que define códigos a ser interpretados por el Núcleo y corresponden a una transacción específica a ejecutar Este campo tiene la siguiente estructura: XXYYZZ XX código para indicar el tipo de transacción. YY Código para indicar el tipo de cuenta que origina la transacción ZZ código para indicar el tipo de cuenta de destino.

DESCRIPCION	I/O	TIPO	LONGIT.	Decimal es	Des de	Hasta	Valores/Restricciones
CódigoCajero	O	A	9		9	17	000000000 Este campo puede ser llenado con nueve ceros.
Código de Oficina	O	A	3		18	20	000 Este campo puede ser llenado con tres ceros
Fecha de la Transacción	O	N	8	0	21	28	YYYYMMDD Ejemplo: 20090122 Corresponde a Enero 22 de 2009.
Hora de la Transacción	O	N	6	0	29	34	HHMMSS Ejemplo: 142510 Corresponde a 14 horas 25 minutos 10 segundos
Fecha Efectiva de la transacción	O	N	8	0	35	42	YYYYMMDD Este campo tiene que tomar el mismo valor del campo Fecha de Transacción en una solicitud.
CódigoCanal	O	A	3		43	45	Valor Fijo= IVR
SwitchCode	O	N	4	0	46	49	Código Numérico que identifica las acciones a ser seguidas en el Núcleo Transaccional

DESCRIPCION	I/O	TIPO	LONGIT.	Decimal es	Des de	Hasta	Valores/Restricciones
Dispositivo	O	A	2		50	51	Valor Fijo= 02(Valor cambiado)
Número Correlativo	O	N	12	0	52	63	Representa un contador para todas las transacciones, el código es puesto en cero todos los días. Puede ser manejado por la aplicación IVR.
Número de Autorización	I	N	6	0	64	69	Puede ser llenado con 000000 para el Mensaje del Módulo API que invoca. El núcleo puede responder con un valor numérico de 6 posiciones
Tipo de Transacción	O	A	1		70	70	1 = Transacción Normal 2 = Transacción Forzada 3 = Reversión de Transacción
Código de Respuesta	I	A	5		71	75	Puede ser llenado con 00099 para el Mensaje del Módulo API que invoca. El núcleo puede responder con un valor numérico de 5 posiciones

DESCRIPCION	I/O	TIPO	LONGIT.	Decimal es	Des de	Hasta	Valores/Restricciones
Descripción del Código de l Respuesta	I	A	75		76	150	Puede ser llenado con 75 blancos para el Mensaje del Módulo API que invoca. El núcleo puede responder con un valor alfanumérico de 75 posiciones relleno con blancos si es necesario.
Relleno	O	A	99		151	250	Puede ser llenado con 99 blancos

[0052] Como se señaló al principio, cada transacción implementa su propia parte variable dependiendo de su naturaleza y funcionalidad.

[0053] La presente invención permite las siguientes transacciones vía interfase de la Parte Fija, la Parte Variable (es decir, la interfase ISO 8583 modificada):

Código de Procesa miento	Descripción	Tipo	Canal de Adquisic ión	Switc h
330000	Consulta de Saldo (Número de Cuenta)	No Monetaria	IVR	2021
330000	Consulta de Saldo (Número de Cuenta)	No Monetaria	WEB	2023
330000	Consulta de Saldo (Número de Cuenta)	No Monetaria	MB	2026
311000	Consulta de Saldo (Número de	No Monetaria	WEB	2023

118

Código de Proceso	Descripción	Tipo	Canal de Adquisición	Switch
	ID)			
311000	Consulta de Saldo (Número de ID)	No Monetaria	MB	2026
330000	Consulta de Saldo (Número de Cuenta)	No Monetaria	SMS	2028
321000	Consulta de Último Movimiento Monetario	No Monetaria	IVR	2021
321000	Consulta de Último Movimiento Monetario	No Monetaria	SMS	2028
321000	Consulta de Último Movimiento Monetario	No Monetaria	WEB	2023
330000	Consulta de Saldo (Número de Cuenta)	No Monetaria	WEB Corporat	2024
330000	Consulta de Saldo (Número de ID)	No Monetaria	WEB Corporat	2024
321000	Consulta de Último Movimiento Monetario	No Monetaria	MB	2026
321000	Consulta de Último Movimiento Monetario	No Monetaria	WEB Corporat	2024
401030	Transferencias a Terceras Partes	Monetaria	IVR	2021
401030	Transferencias a Terceras Partes	Monetaria	WEB	2023
401030	Transferencias a Terceras Partes	Monetaria	MB	2026
500002	Inicio de Sesión	No Monetaria	WEB Corporat	2024
500002	Inicio de Sesión	No Monetaria	WEB	2023

Código de Proceso	miento Descripción	Tipo	Canal de Adquisición	Switch
500002	Inicio de Sesión	No Monetaria	MB	2026
500003	Cambio de PIN de Acceso	No Monetaria	WEB Corporat	2024
500003	Cambio de PIN de Acceso	No Monetaria	WEB	2023
500003	Cambio de PIN de Acceso	No Monetaria	MB	2026
500006	Recuperación de PIN de Acceso (Restablecimiento de Indicador)	No Monetaria	WEB	2023
500006	Recuperación de PIN de Acceso (Restablecimiento de Indicador)	No Monetaria	WEB Corporat	2024
500001	Recuperación de PIN de Acceso (ajuste de PIN)	No Monetaria	WEB Corporat	2024
500001	Recuperación de PIN de Acceso (ajuste de PIN)	No Monetaria	WEB	2023
500007	Recuperación de PIN de Acceso (Restablecimiento de Indicador)	No Monetaria	WEB	2023
500007	Recuperación de PIN de Acceso (Restablecimiento de Indicador)	No Monetaria	Corporat e WEB	2024
330000	Consulta de Saldo # Cuenta/Teléfono Celular	No Monetaria	POS	2014
340000	Consulta de Saldo # Cuenta/Teléfono Celular	No Monetaria	POS	2014
001000	Compra de Bienes y Servicios (Tarjeta)	Monetaria	POS	2014
061001	Compra de Bienes y Servicios (Teléfono Celular)	Monetaria	POS	2014

Código de Proceso	Descripción	Tipo	Canal de Adquisición	Switch
261001	Compra de Bienes y Servicios (Teléfono Celular) Inválida	Monetaria	POS	2014
061002	Verificación IVR PIN Compra de Bienes y Servicios	Monetaria	POS	2014
261002	Verificación IVR PIN Compra de Bienes y Servicios Inválida	Monetaria	POS	2014
201000	Compra de Bienes y Servicios Inválida	Monetaria	POS	2014
021000	Recarga de Cuenta	Monetaria	POS	2014
221000	Recarga de Cuenta Inválida	Monetaria	POS	2014
031000	Redención	Monetaria	POS	2014
231000	Redención Nula	Monetaria	POS	2014

Aplicación de Software de Banco Celular

Funcionalidad

[0054] El Banco Celular o Aplicación de Banca Móvil de la presente invención permite a la NBFi o a los clientes del banco completar transacciones bancarias comunes (por ejemplo, consultas de saldo, transferencias) utilizando un teléfono móvil. Esto permite a la NBFi o a los clientes del banco administrar sus cuentas bancarias desde cualquier ubicación donde haya acceso a señal de teléfono móvil o conexión a Internet.

[0055] La aplicación de Banco Celular de la presente invención puede estar basada en un Midlet J2ME. El Midlet J2ME permite a una NBFi o a los clientes del Banco y al NBFi o al banco comunicarse en una red de datos utilizando una red de datos de operador con conexión telefónica inalámbrica. La aplicación de Banco Celular de la presente invención se comunica con una puerta de entrada de banca móvil para autorizar a un cliente a utilizar la aplicación. La puerta de entrada de banca móvil valida una sesión de usuario y procesa mensajes de entrada y salida

para y desde la Aplicación de Banco Celular. También es responsable por comunicarse con el FEP para enviar mensajes ISO 8583 modificados de las transacciones generadas.

Arquitectura de la Aplicación

[0056] La Aplicación de Banco Celular de la presente invención puede suministrar una serie de aplicaciones integradas configuradas para correr en un esquema de cliente-servidor. En una incorporación, la aplicación de cliente reside en un teléfono móvil de un usuario y adquiere y administra datos que pueden ser necesarios para una transacción en la red del Sistema de Pagos Electrónicos NBFÍ (EPS) de transacciones de bajo valor o un FEP Bancario utilizando la conversión ISO 8583 cuando se ensamblan las transacciones o comunicaciones a la cuenta. La aplicación del cliente utiliza las capacidades de comunicación suministradas por el teléfono móvil para iniciar una conexión de datos con servidores intermediarios que actúan como middleware entre el cliente y la NBFÍ o el banco.

[0057] La arquitectura de conectividad está basada en las características definitorias de los actuales teléfonos móviles, es decir, la capacidad de acceder a la Internet a través de la red celular y transferir datos vía el protocolo HTTP. La arquitectura de comunicación revelada aprovecha la accesibilidad de Internet, transferencia de datos vía el protocolo HTTP, y el creciente poder de cómputo/procesamiento de los teléfonos móviles, para reducir la cantidad de datos intercambiados sobre las plataformas tecnológicas en las que se basa la Aplicación de Banco Celular.

[0058] La Aplicación de Banco Celular de la presente invención puede residir en el teléfono móvil del cliente. La aplicación puede adquirir los datos necesarios para iniciar una transacción desde la red de transacciones de bajo valor. Esos datos pueden traducirse en y enviarse como mensajes cifrados convertidos en código XML. El código XML puede incluir los datos para iniciación de una transacción y pueden ser entregados por middleware al servidor a través de HTTP POST. El middleware traduce los datos reenviados al formato de intercambio de información apropiado utilizando el ISO8583 modificado de la presente invención.

[0059] El código XML utilizado para iniciar cualquier transacción solicitada utiliza una o más etiquetas que pueden ser definidas en términos de los parámetros necesarios a ser incluidos para cada transacción basados en el estándar ISO8583 modificado utilizado en conexión con la red financiera de transacciones de bajo valor. Adicionalmente, para cumplir con los requisitos básicos de seguridad, un programa de criptografía puede ser utilizado para asegurar la información sensible relacionada con las operaciones del sistema financiero de la presente invención. El programa de criptografía puede suministrar protección ligera y robusta sobre la base de encriptación de información sensible como se especifica, por ejemplo, en W3C: XML Encriptación Sintaxis y Procesamiento.

[0060] Es importante tener en cuenta que, preferiblemente, solo cierta información es encriptada por razón de los altos requerimientos computacionales/de procesamiento de encriptación y desencriptamiento de grandes cantidades de datos en un tiempo razonable. Tal encriptación y conversión de mensajes opera en una clave temporal hecha como un polinomio de división variable generado por la sesión FEP, que hace a cada transacción única y diferente de la siguiente. En consecuencia, es preferible generalmente encriptar únicamente datos sensibles como PINs, números de cuenta, etc. Pero en este caso tal encriptación genera menos datos y suministra una resolución única en cada extremo. Esto mejora el desempeño del sistema mientras que añade un valor de seguridad adicional. El servidor de middleware puede ser utilizado para implementar el API 141, por ejemplo. El servidor de middleware también puede tener acceso a una base de datos de sesiones y escribe información en tal base de datos para mantener un seguimiento a las sesiones de comunicación entre los usuarios y el servidor de núcleo. El servidor de middleware también tiene acceso a la base de datos que puede contener información para ayudar a la verificación o validación de cuentas de usuario, por ejemplo. El servidor middleware puede conectar con una base de datos de seguridad que puede contener información que puede ser utilizada para validar los PINs.

Referencias de Flujo de Transacción

[0061] Una característica de la Aplicación de Banco Celular de la presente invención es que esta permite a un cliente iniciar una transacción de compra en un punto de venta suministrando al vendedor únicamente el número de teléfono del cliente y un PIN, por ejemplo.

[0062] Tomando en cuenta las variables que entran en juego en este proceso, la transacción es clasificada por el dispositivo del punto de venta como "Tarjeta No Presente." Esta designación hace una transacción de especial cuidado debido a la potencial exposición al fraude por suplantar al usuario real, y en lo que concierne a los negocios, las transacciones clasificadas como "Tarjeta No Presente" enseguida son verificadas con el cliente. El proceso de verificación puede requerir que el cliente sea contactado por teléfono, en donde se le solicita al cliente que confirme o rechace la transacción, mediante el suministro de un código PIN requerido para las transacciones monetarias.

[0063] Como cada transacción es atómica, esta transacción, que en adelante se define como una transacción en el punto de venta "Referencia", puede dividirse en dos pasos independientes de acuerdo con la presente invención. De acuerdo con una incorporación de la presente invención, en el primer paso, una transacción en el punto de venta es pre-autorizada y se mantiene en el conmutador como pendiente de verificación. En el segundo paso, la transacción en el punto de venta es la auto-verificación del cliente. Así el segundo paso es utilizado para verificar el primer paso. Una vez ejecutados ambos pasos, la transacción "Referencia" en el punto de venta es completada.

[0064] Una forma modificada de la transacción "Referencia" es la transacción "Espera Pasiva". La transacción "Espera Pasiva" también es ejecutada utilizando la red de transacciones de bajo valor de la NBFi o el banco. De acuerdo con una incorporación de la presente invención, la transacción "Espera Pasiva" es similar a la transacción "Referencia" en todos los aspectos excepto que el vendedor en el punto de venta solo se hace consciente de la existencia de la transacción al momento de la transacción.

[0065] La FIG. 9 ilustra un proceso que involucra varias transacciones individuales, en su totalidad, apropiadamente sincronizadas, que son referenciadas como "Referencias."

[0066] La Fig. 9 ilustra tres dispositivos o módulos involucrados en el procesamiento de transacciones que involucran referencias, el POS 1401, el módulo de administración de terminal 1403, y una interfase IVR 1405, la cual puede residir en el módulo de autorización 139 (Fig. 1). Para simplicidad, la Fig. no muestra el proceso de conversión de los mensajes desde el estándar ISO 8583 modificado al estándar ISO 8583.

[0067] En una incorporación el flujo de transacción es como se presenta a continuación:

[0068] 1. Un cliente inicia una transacción de compra utilizando un número de teléfono móvil (no necesita una tarjeta plástica débito o crédito) suministrando todos los datos requeridos para la transacción, incluyendo, por ejemplo, el número de teléfono móvil del cliente 1407. El POS genera un mensaje con la información ID Comerciante internamente programada y una serie de caracteres estándar que incluyen los parámetros de transacción tales como fecha, hora, suma y los auxiliares de los códigos de encriptación de seguridad construidos para Cumplimiento de PCI para otro tipo de transacciones. El mensaje también incluye un código específico que es reconocido por el FEP como una transacción "Referencia". Tal código es parte de la ID de la transacción y se pasa a lo largo del proceso de autorización. El mensaje es enviado al FEP (1451), por ejemplo, al módulo de administración de terminal (1403). El módulo de administración de terminal verifica la suma de la transacción (1409) e identifica la transacción como Transacción Referencia (1411). Al identificar la transacción como una Referencia, el sistema sabe que la realización de la transacción global depende de la verificación de PIN sobre la IVR (1405). Después de la terminación del proceso se presenta un código temporal. Tal código es utilizado para completar el conjunto de todos los parámetros necesarios en la transacción en el POS descrito en el siguiente párrafo.

[0069] 2. El teléfono móvil recibe entonces una solicitud para confirmar la transacción a través del sistema IVR, que solicita al usuario confirmar la transacción con el código de seguridad (PIN1 desde la activación de la cuenta). Una vez recibido y verificado el PIN1 (1413), el IVR comunicará un código de seguridad de un solo uso para que el usuario lo suministre al comerciante. Para

generar un código de seguridad de un solo uso, el administrador del terminal recibe la información del PIN (1419) verifica desde la IVR verifica la vida de la referencia 1421, verifica la información del PIN 1423, y pre-autoriza la transacción 1425. Una vez pre-autorizada se genera un código de pre-autorización y parte de este código puede ser utilizado como el código de seguridad de un solo uso (PIN2).

[0070] 3. Se le envía al vendedor en el punto de venta un mensaje 1453 referenciando la transacción pendiente 1415 junto con una señal de espera 1417, que puede ser mostrada en un monitor o pantalla en el POS. Este mensaje es enviado por el FEP como respuesta a la solicitud de transacción Referencia. La señal de espera puede incluir un mensaje amistoso tal como "Procesando Por favor espere." Al momento en el que la señal de espera es recibida por el vendedor en el punto de venta, los datos necesarios para iniciar el segundo paso de la transacción 1455 han sido enviados por confirmación por el FEP. Este segundo paso puede iniciarse si existe uno de estos dos eventos:

- El cliente ya ha comprobado exitosamente el PIN1 sobre el IVR, para que el cliente pueda aconsejar al vendedor en el punto de venta presionar una tecla o una tecla programada en el monitor que indique "Espera Pasiva," por ejemplo. Presionando la tecla programada "Espera Pasiva" puede ser el desencadenante para el vendedor en el punto de venta para comunicar la respuesta de los datos de verificación de la transacción 1455 recibida como resultado de la primera solicitud de transacción "Referencia".

- El tiempo de espera predeterminado para "espera pasiva" ha caducado, por lo que el punto de venta se convierte en desbloqueado mediante el envío de 1455 los datos de respuesta recibidos de la primera solicitud de transacción "Referencia" para determinar si la transacción puede ser verificada.

4. En ese momento la verificación del PIN ha sido comunicada por el usuario/cliente a través del teléfono móvil, independientemente de que el evento ocurra en el paso anterior tres. Se le pedirá al administrador del terminal verificar si la transacción fue validada por el comerciante con el PIN2 1427 (En una incorporación el IVR suministra PIN2 al cliente y el cliente en retorno suministra PIN2 al comerciante). Este paso involucra las siguientes alternativas:

- El FEP verifica que el comerciante ha suministrado el PIN2 correcto y la transacción es aprobada finalmente. El FEP entonces comunica al vendedor 1431 en el punto de venta que la transacción se aprobó y puede imprimirse un recibo

1433.

- El FEP rechaza la transacción porque el comerciante no suministró un PIN2 correcto. El FEP entonces se comunica con el vendedor 1431 en el punto de venta donde la transacción ha sido rechazada y un recibo de rechazo apropiado puede ser impreso 1433.

La anterior descripción de las posibles implementaciones consistentes con la presente invención no representan una lista completa de todas las implementaciones o todas las variaciones de implementaciones descritas. La descripción de únicamente algunas de las implementaciones no debe interpretarse como un intento de excluir otras implementaciones. Por ejemplo, los expertos entenderán como implementar la invención de muchas otras formas, utilizando equivalentes y alternativas que no se aparten del ámbito de la invención. Además, a menos que se indique lo contrario en la descripción precedente, ninguno de los componentes descritos en las implementaciones son esenciales para la invención. Por lo tanto, se pretende que la especificación y los ejemplos sean considerados como ejemplificantes solamente, con un verdadero alcance y espíritu de la invención indicada por las siguientes reivindicaciones.

REIVINDICACIONES

Lo que se Reivindica es:

1. Un sistema para procesamiento electrónico de transacciones financieras que comprende: Al menos un dispositivo remoto para el montaje de los mensajes de datos en un primer formato, los mensajes de datos incluyen solicitudes de autorización para realizar transacciones financieras sin tarjeta basadas en el uso de un número de teléfono móvil como una referencia a una cuenta de usuario (o una combinación de número de acceso, la selección al responder a múltiples cuentas o productos financieros vinculados al número Telefónico); una aplicación de interfase de programa que reside en un servidor para recibir y convertir dichos mensajes de datos en un segundo formato; un modulo adquiriente que adquiere y decodifica instrucciones en los mensajes de datos que tienen un segundo formato; y un modulo de procesamiento para ejecutar instrucciones adquiridas por el modulo adquiriente para leer o escribir información en una base de datos back end; en donde el modulo adquiriente además se comunica con el dispositivo remoto para informar al dispositivo remoto si la transacción financiera solicitada ha sido aprobada.
2. El sistema de la reivindicación 1, en donde el módulo adquiriente incluye un módulo de autorización o un módulo de transacción.
3. El sistema de la reivindicación 2, donde el dispositivo remoto incluye un dispositivo de punto de venta o una caja registradora electrónica y el módulo adquiriente incluye un módulo de administración de terminal para el procesamiento de solicitudes desde el dispositivo de punto de venta o la caja registradora electrónica.
4. El sistema de la reivindicación 2, en donde el módulo de autorización verifica: Si una cuenta a ser debitada tiene el suficiente saldo para completar la transacción solicitada; Si un PIN ingresado en un dispositivo remoto coincide

con un PIN almacenado en la base de datos backend; o Si un número de autorizaciones es cumplido.

5. El sistema de la reivindicación 2, en donde el modulo de autorización emite un código temporal a ser utilizado como un token de seguridad en la realización de transacciones financieras.

6. El sistema de la reivindicación 5, en donde el código temporal comprende los dos últimos dígitos de una ID de sesión.

7. El sistema de la reivindicación 1, en donde el primer formato es ISO 8583 modificado para incluir una parte fija y una parte variable.

8. Un método para procesamiento de transacciones electrónicas que comprende la creación de una cuenta de usuario, el método comprende: Recibir un número de teléfono celular asociado con un nuevo usuario; Activar una llamada a través de un sistema de respuesta de voz interactivo para verificar la identificación del usuario y la propiedad del teléfono celular por tal usuario; Recibir a través de un punto de venta un número de identificación personal del nuevo usuario; Configuración de una nueva cuenta de usuario; Recibir, a través del punto de venta, una suma de depósito y el número de teléfono celular del usuario; Generar un código temporal y comunicar dicho código al punto de venta; Recibir el código temporal a través del punto de venta; y Financiación de la cuenta de usuario.

9. El método de la reivindicación 8, además comprende la transmisión de un mensaje de texto al usuario para confirmar que la cuenta ha sido configurada y financiada.

10. Un método para transferir efectivo desde una primera cuenta de usuario a una segunda cuenta de usuario, el método comprende: Recibir el número celular asociado con la cuenta del segundo usuario, la suma de la transferencia y el número de identificación personal asociado con la cuenta del primer usuario;

Validar el número de teléfono celular recibido y la cuenta del segundo usuario en un CMS; Validar el número de autorizaciones de cuenta de primer usuario en el CMS; Recibir en una interfase de aplicación de programa una solicitud para transferencia en un primer formato; Convertir la solicitud a un segundo formato y enviar el mensaje convertido a un módulo de autorización; Crear en el modulo de autorización un código temporal si el primer usuario tiene los fondos suficientes; y Acreditar en la cuenta del segundo usuario.

11. El método de la reivindicación 10, además comprende: transmitir un mensaje de texto al primer usuario para confirmar que la transferencia está completa.

12. Un método para retirar efectivo de un ATM que comprende: Recibir una solicitud en un primer formato por el titular de la cuenta para retirar efectivo del ATM; Recibir un número de teléfono celular del titular de la cuenta; Verificar en el modulo de procesamiento front end si la solicitud es aceptada o declinada con base en el número de teléfono celular y los fondos disponibles en la cuenta del titular; Transmitir el código temporal al titular de la cuenta; Recibir de la ATM una solicitud en un primer formato que incluye el código temporal, el número de teléfono celular del titular de la cuenta, y el código de identificación del usuario; Transmitir al servidor de la institución financiera una solicitud en un segundo formato para dispensar efectivo; y Recibir autorización de dicho servidor para retirar el efectivo.

13. El método de la reivindicación 12, en donde dicho primer formato es un mensaje ISO 8583 modificado con una parte fija y una parte variable y dicho segundo formato es un mensaje ISO 8583.

14. El método de la reivindicación 12, además comprende transmitir un mensaje de texto al titular de la cuenta para confirmar la transacción de dispensar efectivo.

15. Un método para procesamiento electrónico de compras en un punto de venta que comprende: Recibir en una interfase de aplicación de programa, un mensaje en un primer formato desde un punto de venta que incluye un número celular de usuario y un valor de compra; Convertir dicho mensaje en el primer formato en un mensaje en un segundo formato; En el modulo de procesamiento de front end, recibir dicho mensaje en un segundo formato y encontrar parámetros dentro de dicho mensaje en un segundo formato; Iniciar una rutina de interfase de voz en un módulo de interfase de voz; Realizar una llamada al usuario utilizando la rutina de interfase de voz y obteniendo autorización del usuario para la transacción de compra una vez el usuario ingrese su Numero Personal de Identificación; Transmitir un código temporal al punto de venta; Recibir, en una interfase de aplicación de programa, un segundo mensaje en un primer formato desde el punto de venta que incluya una solicitud de renovación de la transacción de compra, la solicitud renovada incluyendo el código temporal; y Autorizar la transacción de compra.

16. El método de la reivindicación 15, en donde dicho primer formato es un mensaje ISO 8583 modificado con una parte fija y una parte variable y dicho segundo formato es un mensaje ISO 8583.

17. Un método para procesamiento electrónico de desembolsos de nómina que comprende: Recibir autorización del empleador para pago de nómina con uno o dos tokens de seguridad; Verificar que la cuenta del empleador esté activa y que el empleador no haya excedido el número de autorizaciones; Recibir el pago de nómina solicitado en un primer formato; Convertir la solicitud en un segundo formato; Autorizar el pago de nómina si la cuenta del empleador tiene saldo suficiente y el número de autorizaciones no ha sido excedido; y Acreditar en la cuenta del empleado.

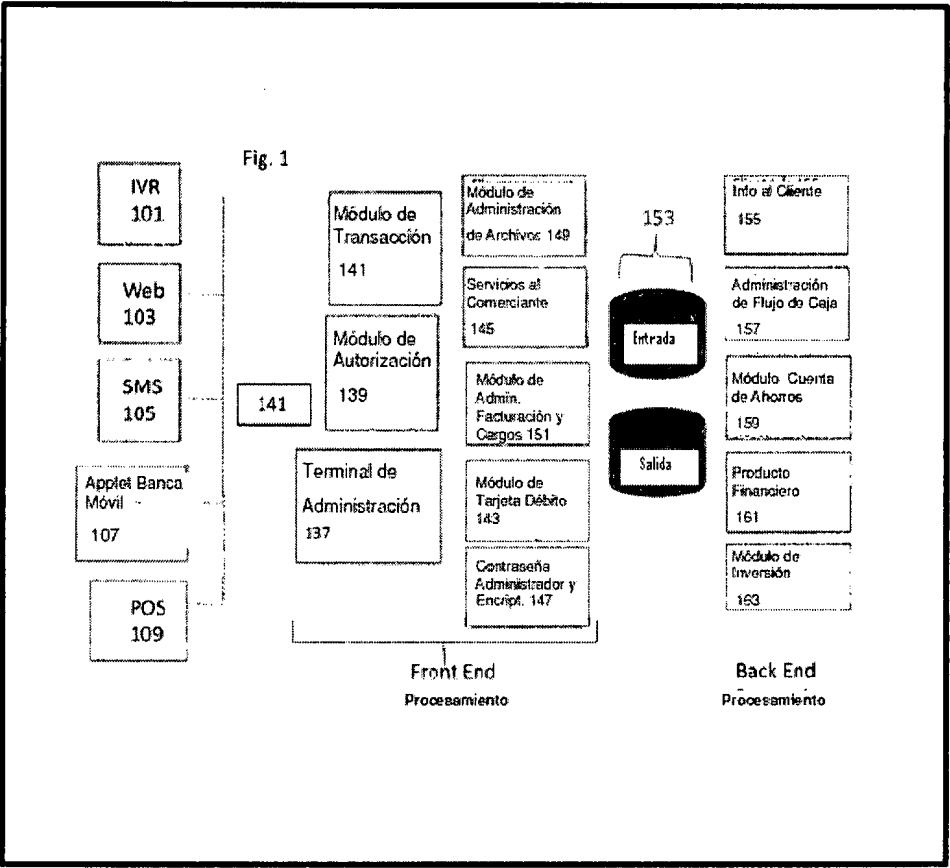
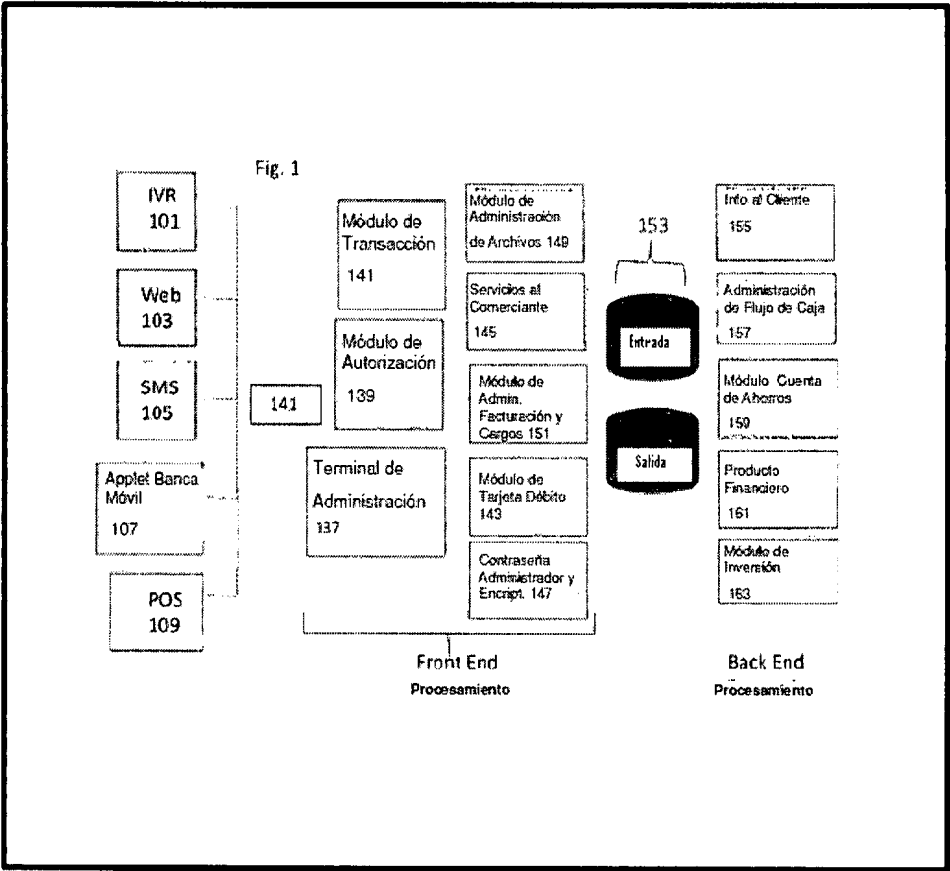
18. El método de la reivindicación 17, en donde dicho primer formato es un mensaje ISO 8583 modificado con una parte fija y una parte variable y dicho segundo formato es un mensaje ISO 8583.

19. Un método para el procesamiento electrónico de pagos a beneficiarios que comprende: Recibir un mensaje de un teléfono celular en un primer formato que incluye una solicitud de pago a un beneficiario, el mensaje incluye el número de teléfono celular de un solicitante, el código de identificación del solicitante, la identificación de un beneficiario, y una suma de pago; Convertir el mensaje en un segundo formato; Autorizar el pago si la cuenta del solicitante tiene saldo suficiente, un número de autorizaciones no es excedido, y el código de identificación es válido; y Acreditar en la cuenta del beneficiario.

20. El método de la reivindicación 19, en donde dicho primer formato es un mensaje ISO 8583 modificado con una parte fija y una parte variable y dicho segundo formato es un mensaje ISO 8583.

RESUMEN

[0071] Los sistemas y métodos de la presente invención incluyen una arquitectura de sistema integral que permite el acceso a instituciones financieras no bancarias (NFBIs) y bancos a través de dispositivos en punto de venta y teléfonos móviles, por ejemplo. La presente invención involucra el uso de un estándar ISO 8583 modificado para permitir a los usuarios hacer interfase con un sistema de procesamiento de front end directamente desde los dispositivos no tradicionales. La presente invención también permite banca móvil con los NBFIs a través del uso de una aplicación que reside en un teléfono móvil de un usuario, que permite el encapsulamiento de información del usuario como XML, por ejemplo, y la transmisión de ellos sobre http mientras cumple con el estándar ISO 8583, y además permite la encriptación de ciertos datos de usuario, sin que tenga que recurrir al acceso a la página web de banca móvil. En un aspecto de la invención, una aplicación POS puede ejecutarse en la parte superior de PCI para permitir a los usuarios hacer compras utilizando fondos pre-depositados en una cuenta NBFIs.





No. 12-121806-00000-0000

Fecha: 2012-07-19 13:34:03 Dep. 2020 DIR.NUEVASCR
Tra. 2 PATENTES Eve. 1 REGDEPOSITO
Act. 411 PRESENTACION Folios: 133
Act. 411 PRESENTACION Folios: 135

IES

PATENTE DE INVENCION ☒

MODELO DE UTILIDAD ☐

36/00

☒	Indicación que se 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 el caso formato de descuento)
Completa ☒	Incompleta ☐

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

☐	Indicación que se solicita una PCT
☐	Copia de la solicitud en español, tal como fue presentada inicialmente (capítulo descriptivo, reivindicatorio, resumen)
☐	Dibujos de ser estos pertinentes
☐	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 DE 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 gráfica de un esquema de trazado
☐	Comprobante de pago de las tasas establecidas
Completa ☐	Incompleta ☐