



No. 13-169786- -00000-0000

Fecha: 2013-07-17 16:53:00
Tra. 11 PATENTE IYII
Act. 411 PRESENTACION

Dep. 2020 DIR.NUEVASCR
Eve: 378 FASE NACIONAL I
Folios: 49

DELEGATURA PROPIEDAD INDUSTRIAL

División de Nuevas Creaciones

SOLICITUD
PATENTE DE INVENCION

ENTRADA EN FASE NACIONAL

21. **EXPEDIENTE No.** _____

SISTEMA DE PAGO EN EL SURTIDOR DE COMBUSTIBLE PARA ASEGURAR

54. **TITULO** _____
LA EVALUACIÓN DE LOS DATOS DEL TITULAR DE LA TARJETA

51. **CLASIFICACION INTERNACIONAL** _____

71. **SOLICITANTE** _____
GILBARCO INC. y GILBARCO, S.R.L.

DOMICILIO _____
GREENSBORO, NC, ESTADOS UNIDOS DE AMÉRICA y
FLORENCE, ITALIA

74. **APODERADO** _____
JUAN PABLO CADENA SARMIENTO

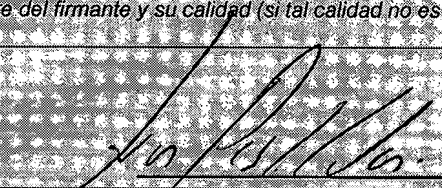
22. **BOGOTÁ, D.C.** _____

 Industria y Comercio SUPERINTENDENCIA	SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO  No. 13-169786- -00000-0000 Fecha: 2013-07-17 16:53:00 Dep. 2020 DIR.NUEVASCR Tra. 11 PATENTEIYII Eve: 378 FASENACIONALI Act. 411 PRESENTACION Folios: 49 Radicación
---	--

AS. 125.085

DIRECCIÓN DE NUEVAS CREACIONES
SOLICITUD FASE NACIONAL –PCT

1	TIPO DE SOLICITUD	☒ Patente de invención ☒ Capítulo I	☐ Patente de Modelo de Utilidad ☐ Capítulo II	
2	DATOS SOLICITUD INTERNACIONAL PCT (86)			
Solicitud Internacional No.		PCT/US2011/066203	Fecha	20.12.2011
Publicación Internacional No.		WO 2012/088135	Fecha	28.06.2012
3	TÍTULO DE LA INVENCIÓN (200 caracteres o espacios máximos)			
SISTEMA DE PAGO EN EL SURTIDOR DE COMBUSTIBLE PARA ASEGURAR LA EVALUACIÓN DE LOS DATOS DEL TITULAR DE LA TARJETA				
4	CLASIFICACIÓN INTERNACIONAL (CIP)			
5	SOLICITANTE (S) ☐ Esta persona también es inventor. Para datos adicionales utilizar hoja de información complementaria			
APELLIDOS O RAZÓN SOCIAL		NOMBRE	IDENTIFICACIÓN	TIPO
1. GILBARCO INC.				
6	DATOS DEL SOLICITANTE			
DIRECCIÓN		7300 West Friendly Avenue, 27420	No. TELÉFONO	
CIUDAD		Greensboro	CORREO ELECTRÓNICO	
DEPARTAMENTO/ESTADO		NC	NACIONALIDAD O US	
PAÍS DE RESIDENCIA		US	LUGAR DE CONSTITUCIÓN	
7	INVENTOR (ES) Para datos adicionales utilizar hoja de información complementaria			
APELLIDOS		NOMBRES	NACIONALIDAD	
1. CARAPELLI		Giovanni	IT	
2. RINGEMAN		Kenneth	US	
3. WILLIAMS		Rodger	US	
DIRECCIÓN DE CORREO ELECTRÓNICO:				
8	DATOS INVENTOR (ES)			
PAÍS RESIDENCIA		DEPARTAMENTO/ESTADO	CIUDAD	DIRECCIÓN
1. IT			Florence	via L. Adreotti 73, I-50142
2. US		NC	Kernersville	421 Drayton Park, 27284
3. US		NC	Siler City	9743 Silk Hope Liberty Road, 27344
OTRO(S) SOLICITANTE(S) Y/O (OTRO(S)) INVENTOR(ES)				
☒ Los demás solicitantes y/o (demás) inventores se indican en una hoja de información complementaria.				
9	☐ REPRESENTANTE LEGAL ☒ APODERADO			
APELLIDOS		NOMBRES	IDENTIFICACIÓN	
CADENA SARMIENTO		JUAN PABLO	C.C . 80.410.337 T.P . 57492	
DIRECCIÓN		Calle 70A 4 41	No. TELÉFONO 7442200	
CIUDAD		Bogotá, D.C.	CORREO ELECTRÓNICO	
PAÍS		CO	No. RADICACIÓN O PROTOCOLO DE PODER GENERAL	
10	DECLARACIONES DE PRIORIDAD ☒ SI ☐ NO			
(33) PAÍS DE ORIGEN		CÓDIGO PAÍS	(31) NÚMERO	(32) FECHA (AAAA/MM/DD)
1. US		US	12/975,502	2010/12/22
2.				
3.				

11	DECLARACIÓN SOBRE USO DE RECURSOS GENÉTICOS O BIOLÓGICOS		
<i>Declaro que el objeto de la presente solicitud de patente fue obtenido a partir de recursos genéticos o biológicos de los que cualquiera de los países miembros de la Comunidad Andina es país de origen.</i>			
☐ SI ☒ NO			
Nota: En caso afirmativo deberá anexar copia del contrato de acceso de recursos genéticos o productos derivados, o certificado o número de registro, expedido por la Autoridad competente.			
12	DECLARACIÓN SOBRE USO DE CONOCIMIENTOS TRADICIONALES		
<i>Declaro que el objeto de la presente solicitud de patente fue obtenido a partir de conocimientos tradicionales de comunidades indígenas, afroamericanas o locales de países miembros de la Comunidad Andina.</i>			
☐ SI ☒ NO			
Nota: En caso afirmativo deberá anexar la licencia o autorización de uso de conocimiento tradicional, o certificado o número de registro.			
13	REDUCCIÓN DE TASAS		
<i>Declaro que carezco de medios económicos para presentar la solicitud de patente.</i>			
☐ SI ☒ NO			
Nota: En caso de ser persona natural y carecer de medios económicos, y por lo tanto, aplique la reducción de tasas a que se refiere la resolución vigente en tarifas, debe firmar la presente solicitud bajo la gravedad de juramento.			
Micro, pequeñas y medianas empresas ☐			
Universidades públicas o privadas ☐			
Entidades sin ánimo de lucro ☐			
Debe aportar los documentos que se indican en el numeral 17 de anexos			
14	AUTORIZACIÓN DE NOTIFICACIÓN EN LÍNEA ☒ SI ☐ NO		
Manifiesto que he leído y entendido perfectamente los términos y condiciones de uso de medios electrónicos para las notificaciones en línea a través de Internet de los actos administrativos proferidos por la Superintendencia de Industria y Comercio que deben ser notificados personalmente y, en consecuencia, autorizo el servicio de notificación a través de internet.			
15	COMPROBANTE DE PAGO O PAGO ELECTRÓNICO	No. 13-54513, 13-38199, 13-46829	Fecha: 10.07.2013
16	FIRMA DEL SOLICITANTE, DEL APODERADO O DEL REPRESENTANTE LEGAL <i>Junto a cada firma, indicar el nombre del firmante y su calidad (si tal calidad no es obvia al leer el petitorio)</i>		
			
17	ANEXOS		
Documentación Técnica Solicitud Internacional en castellano		Documentación Jurídica	
1. ☒ Descripción N° de folios: 6-32		9. ☐ Poderes, si fuera el caso.	
2. ☒ Reivindicaciones N° Reivindicaciones: 35		10. ☐ Documento que legalmente pruebe la cesión del inventor al solicitante o a su causante.	
3. ☒ Dibujos y/o figuras N° folios: 41-46		11. ☐ Copia del contrato de acceso de recursos genéticos o productos derivados, certificado o número de registro, si fuera el caso.	
4. ☒ Resumen.		12. ☐ Copia de la licencia o autorización de Conocimientos Tradicionales, certificado o número de registro, si fuera el caso.	
5. ☐ Certificado de depósito de material biológico si fuera el caso.		13. Reducción de tasas	
6. ☐ Listado de secuencias de nucleótidos y/o aminoácidos en forma digital si fuera el caso.		Micro, pequeñas o medianas empresas	
7. ☐ Arte final 12 x 12.		☐ Copia simple de la declaración de renta del año inmediatamente anterior, o en su defecto prueba documental idónea.	
8. ☐ Anexo formato digital.		☐ Documento de constancia de cumplimiento con lo establecido en la ley 905 de 2004.	
		Universidades públicas o privadas	
		☐ Copia acto de reconocimiento institucional emitido por el Ministerio de Educación	
		Entidades sin ánimo de lucro	
		☐ Copia de registro vigente en Cámara de comercio.	
		☒ Hoja de información complementaria.	
		☐ Otros, especificar:	
		14. ☒ Comprobante de pago de la tasa de presentación de la solicitud.	
		15. ☐ Comprobante de pago por reivindicación de prioridad.	
		16. ☐ Comprobante de pago de la tasa por concepto de excedente de palabras en la publicación.	
		17. ☒ Comprobante de pago por reivindicación adicional a 10.	

1	(12) TIPO DE SOLICITUD		NUMERO DE RADICACIÓN	
☒ Patente de invención		FECHA DE PRESENTACIÓN		
☐ Patente de Modelo de Utilidad				
4	(71) SOLICITANTE (S)			
APELLIDOS O RAZÓN SOCIAL		NOMBRE	IDENTIFICACIÓN	TIPO
2.	GILBARCO, S.R.L.			
3.				
4.				
5	DATOS DEL SOLICITANTE			
PAÍS DE RESIDENCIA		DEPARTAMENTO/ESTADO	CIUDAD	DIRECCIÓN
2.	IT		Florence	Via de' Cattani 220/G, I-50145
3.				
4.				
TELÉFONO		FAX	E-MAIL	NACIONALIDAD
2.				ES
3.				
4.				
6	(72) INVENTOR (ES)			
APELLIDOS		NOMBRE	NACIONALIDAD	
5.				
6.				
7.				
8.				
9.				
10.				
7	DATOS INVENTOR (ES)			
DIRECCIÓN		CIUDAD	DEPARTAMENTO/ESTADO	PAÍS RESIDENCIA
5.				
6.				
7.				
8.				
9.				
10.				
9	(30) DECLARACIONES DE PRIORIDAD			
PAÍS DE ORIGEN		CÓDIGO PAÍS	NÚMERO	FECHA (AAAA/MM/DD)
4.				
5.				
6.				
7.				
8.				
9.				
10.				

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
28 June 2012 (28.06.2012)



(10) International Publication Number
WO 2012/088135 A1

- (51) International Patent Classification:
G06Q 20/00 (2012.01)
- (21) International Application Number:
PCT/US2011/066203
- (22) International Filing Date:
20 December 2011 (20.12.2011)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
12/975,502 22 December 2010 (22.12.2010) US
- (71) Applicants (for all designated States except US): **GILBARCO INC.** [US/US]; 7300 West Friendly Avenue, Greensboro, North Carolina 27420 (US). **GILBARCO, S.R.L.** [IT/IT]; Via de' Cattani 220/G, I-50145 Florence (IT).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **CARAPPELLI, Giovanni** [IT/IT]; via L. Adreotti 73, I-50142 Florence (IT). **RINGEMAN, Kenneth** [US/US]; 421 Drayton Park, Kernersville, North Carolina 27284 (US). **WILLIAMS, Rodger** [US/US]; 9743 Silk Hope Liberty Road, Siler City, North Carolina 27344 (US).
- (74) Agents: **KILLEN, Craig N.** et al.; Nelson Mullins Riley & Scarborough LLP, 100 North Tryon Street, 42nd Floor, Charlotte, North Carolina 28202 (US).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

[Continued on next page]

(54) Title: FUEL DISPENSING PAYMENT SYSTEM FOR SECURE EVALUATION OF CARDHOLDER DATA

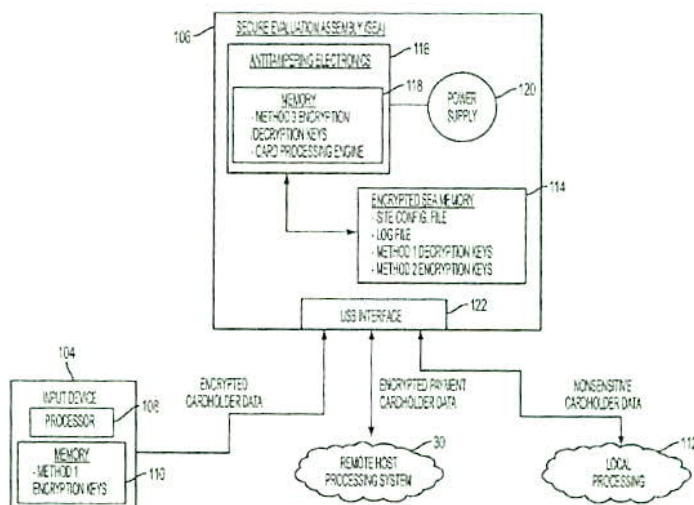


FIG. 4

(57) Abstract: A system used in a retail environment for providing end-to-end encryption of payment cardholder data. An input device configured to receive cardholder data is operative to encrypt the cardholder data according to a first encryption method to produce first encrypted cardholder data. A cardholder data handling device is in electronic communication with the input device. A secure evaluation assembly (SEA) is operatively connected to the cardholder data handling device and comprises antitampering control electronics adapted to decrypt the first encrypted cardholder data to produce unencrypted cardholder data. The antitampering control electronics evaluate the unencrypted cardholder data to determine whether the unencrypted cardholder data is payment cardholder data or nonsensitive cardholder data. Finally, if the unencrypted cardholder data is payment cardholder data, the antitampering control electronics of the SEA are adapted to encrypt the unencrypted cardholder data according to a second encryption method to produce second encrypted cardholder data.

WO 2012/088135 A1

WO 2012/088135 A1



-
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

SISTEMA DE PAGO EN EL SURTIDOR DE COMBUSTIBLE PARA ASEGURAR LA EVALUACIÓN DE LOS DATOS DEL TITULAR DE LA TARJETA

CAMPO DE LA INVENCION

La presente invención está relacionada, generalmente, con el expendio de combustible y con otros sistemas de pago al por menor. Más particularmente, la invención está relacionada con un dispositivo y un método para la creación de un sistema de evaluación segura, en un terminal al por menor o de punto de venta (POS), y evaluando de forma segura una comunicación encriptada desde el terminal o desde el punto de venta hacia un computador central.

ANTECEDENTES DE LA INVENCION

Los sistemas de pago han sido incorporados dentro de las estaciones de combustible, con el fin de permitir a un cliente de pagar por el combustible y otras mercancías y servicios (tal como los alimentos y los productos de la tienda de conveniencia), usando una tarjeta de crédito o de débito. Las tarjetas de cliente o las tarjetas específicas del programa, que da derecho al cliente a un crédito prefijado o un descuento porcentual, u otras condiciones de precios favorables también son típicamente aceptadas.

Tales sistemas de pago comprenden varios dispositivos de entrada, tal como los lectores de tarjeta y los teclados de PIN, que están configurados para aceptar los datos necesarios para procesar el pago. El cliente puede proveer ciertos datos de pago deslizando una tarjeta de pago, portando una banda magnética, a través de un lector de tarjetas. Los datos almacenados en la banda magnética pueden incluir un Número de Cuenta Primaria (PAN), el nombre del titular de la tarjeta, un código de servicio y la fecha de vencimiento de la tarjeta. También, si es requerido para completar la transacción, el cliente puede entrar un número de identificación personal (PIN) usando un teclado de PIN. El sistema comunica los datos a un sistema anfitrión remoto responsable para la verificación respecto a la cuenta del cliente.

Debido al continuado desafío que el fraude plantea a los clientes, comerciantes y a los bancos, entre otros, las compañías de tarjetas de pago están requiriendo más y más seguridad durante las transacciones con tarjetas de pago. Por ejemplo, las organizaciones que procesan, almacenan o transmiten datos del

titular de la tarjeta de pago, deben cumplir con ciertos estándares industriales. Los comerciantes y los proveedores de servicios deben demostrar el cumplimiento con los estándares sobre una base recurrente, un proceso costoso y complejo.

Un método para el procesamiento y la transmisión de los datos del titular de la tarjeta de pago, es conocido como la encriptación de extremo a extremo (E2EE). En una implementación típica de E2EE, los datos del titular de la tarjeta son encriptados en un dispositivo de entrada, y permanecen encriptados hasta que alcancen su destinación prevista (usualmente, un computador central). Los datos del titular de la tarjeta de pago nunca están accesibles a un comerciante en forma de texto claro, cuando pasan a través de los componentes de sistemas intermediarios.

Aunque el uso de la E2EE provee un alto nivel de seguridad para los datos del titular de la tarjeta de pago, presenta ciertos problemas para los comerciantes. Por ejemplo, los comerciantes requieren porciones de los datos del titular de la tarjeta de pago para los propósitos de reconciliación. Sin embargo, es un sistema empleando la E2EE, los comerciantes no pueden acceder a los datos del titular de la tarjeta después de que son encriptados en un dispositivo de entrada. Por consiguiente, si un cliente reclama una transacción, el comerciante no puede verificar el PAN, con el fin de probar que la transacción tuvo lugar. De igual modo, el comerciante no puede dar crédito a una cuenta del cliente, o completar manualmente una transacción que previamente se rechazó debido a un error.

Además, los estándares industriales que regulan las transacciones de tarjetas de pago, típicamente, no se aplican a los datos no sensibles del titular de la tarjeta de las otras tarjetas, procesadas *in situ*, o en una red privada del mercado minorista, tal como los datos de una tarjeta de cliente o las tarjetas de programa específico. Sin embargo, en un sistema de E2EE, estos datos son encriptados en el dispositivo de entrada junto con los datos del titular de la tarjeta de pago. Por consiguiente, por ejemplo, el comerciante no puede acceder a los datos de la tarjeta de cliente con el fin de dar crédito al cliente para una transacción.

RESUMEN DE LA INVENCION

La presente invención reconoce y aborda las desventajas de las construcciones y los métodos del estado actual del arte. En un aspecto, la presente invención provee un sistema usado en un entorno minorista, para proveer la encriptación de extremo a extremo de los datos del titular de la tarjeta de pago. El sistema comprende un dispositivo de entrada configurado para recibir los datos del titular de la tarjeta. El dispositivo de entrada está operativo para encriptar los datos del titular de la tarjeta, de acuerdo con un primer método de encriptación, con el fin de producir los primeros datos encriptados del titular de la tarjeta. El sistema también comprende un dispositivo de manipulación de los datos del titular de la tarjeta, en comunicación electrónica con el dispositivo de entrada. Un sistema de evaluación está operativamente conectado con el dispositivo de manipulación de los datos del titular de la tarjeta, y el sistema de evaluación segura comprende la electrónica de control respecto a la manipulación indebida, adaptada para desencriptar los primeros datos encriptados del titular de la tarjeta, con el fin de producir los datos no encriptados del titular de la tarjeta. La electrónica de control respecto a la manipulación indebida del sistema de evaluación segura, evalúa los datos no encriptados del titular de la tarjeta, con el fin de determinar si los datos no encriptados del titular de la tarjeta son los datos del titular de la tarjeta de pago, o los datos no sensibles del titular de la tarjeta. Finalmente, si los datos no encriptados del titular de la tarjeta son los datos del titular de la tarjeta de pago, la electrónica de control respecto a la manipulación indebida del sistema de evaluación segura, es adaptada para encriptar los datos no encriptados del titular de la tarjeta, de acuerdo con un segundo método de encriptación, con el fin de producir los segundos datos encriptados del titular de la tarjeta.

De acuerdo con un aspecto ulterior, la presente invención provee un sistema de evaluación segura, en la cual una comunicación encriptada de los datos del titular de la tarjeta, desde un dispositivo de entrada hasta un sistema procesador anfitrión remoto, puede ser evaluado de forma segura. El sistema de evaluación segura comprende la electrónica de control respecto a la manipulación indebida, y una memoria del sistema de evaluación segura. La memoria del sistema de evaluación segura contiene la información necesitada para desencriptar los datos encriptados, de acuerdo con un primer método de encriptación, y la información necesitada para encriptar los datos, de acuerdo con un segundo método de encriptación. Además, la memoria del sistema de evaluación segura está encriptada de acuerdo con un tercer método de

encriptación. La electrónica de control respecto a la manipulación indebida está adaptada para desenscriptar la memoria del sistema de evaluación segura, y está adaptada ulteriormente para desenscriptar los datos del titular de la tarjeta, encriptados de acuerdo con el primer método de encriptación, con el fin de producir los datos no encriptados del titular de la tarjeta. Finalmente, la electrónica de control respecto a la manipulación indebida está adaptada, ulteriormente, para evaluar los datos no encriptados del titular de la tarjeta, y encriptar los datos no encriptados del titular de la tarjeta, de acuerdo con el segundo método de encriptación, si los datos no encriptados del titular de la tarjeta son los datos del titular de la tarjeta de pago.

En un aspecto ulterior, la presente invención provee un método para el procesamiento de una transacción, involucrando los datos del titular de la tarjeta en un sistema de pago minorista. El método comprende la recepción de los datos del titular de la tarjeta en un dispositivo de entrada, y la encriptación de los datos del titular de la tarjeta, de acuerdo con un primer método de encriptación, con el fin de producir los primeros datos encriptados del titular de la tarjeta. El método comprende, además, la recepción de los primeros datos encriptados del titular de la tarjeta en un sistema de evaluación segura, acoplado a un dispositivo de manipulación de los datos del titular de la tarjeta, y la desenscriptación de los primeros datos encriptados del titular de la tarjeta, con el fin de producir los datos no encriptados del titular de la tarjeta. En adición, el método comprende la evaluación de los datos no encriptados del titular de la tarjeta, en una electrónica de control respecto a la manipulación indebida, con el fin de determinar si los datos no encriptados del titular de la tarjeta son los datos del titular de la tarjeta de pago, o los datos no sensibles del titular de la tarjeta. Finalmente, el método comprende la encriptación de los datos no encriptados del titular de la tarjeta, de acuerdo con un segundo método de encriptación, con el fin de producir los segundos datos encriptados del titular de la tarjeta, si los datos no encriptados del titular de la tarjeta son los datos del titular de la tarjeta de pago.

Aquellas personas experimentadas en el arte apreciarán el alcance de la presente invención, y se darán cuenta de aspectos adicionales de ellos, después de leer la siguiente descripción detallada de las puestas en práctica preferidas, en asociación con las figuras de los dibujos acompañantes.

BREVE DESCRIPCION DE LOS DIBUJOS

Una revelación completa y reproducible de la presente invención, incluyendo el mejor modo de ella dirigida a una de las personas experimentadas en el arte, es expuesta en la especificación, la cual hace referencia a los dibujos anexados, en los cuales:

La Figura 1 es una ilustración esquemática de un entorno minorista de expendio de combustible, el cual puede utilizar una puesta en práctica de la presente invención.

La Figura 2 es una vista frontal en elevación de un surtidor de combustible ejemplar que puede operar con un dispositivo POS (punto de venta) y/o un controlador de sitio dentro del entorno minorista de carga de combustible de la Figura 1.

La Figura 3 es una ilustración diagramática de un sistema de pago que tiene un sistema de evaluación segura, de acuerdo con una puesta en práctica de la presente invención.

La Figura 4 es una ilustración esquemática de un sistema de evaluación segura, adaptado para la evaluación de los datos del titular de la tarjeta, transmitidos desde un dispositivo de entrada hacia un sistema procesador anfitrión remoto, de acuerdo con una puesta en práctica de la presente invención.

La Figura 5 es un diagrama de flujo ilustrando un método ejemplar para el procesamiento de una transacción, involucrando los datos del titular de la tarjeta usando el sistema de la Figura 4.

La Figura 6 es un diagrama de flujo ilustrando un método ejemplar para el procesamiento de una solicitud, con el fin de validar una transacción involucrando datos del titular de la tarjeta de pago, usando el sistema de la Figura 4.

El uso repetido de los caracteres de referencia en la especificación y los dibujos presentes, está previsto para representar los mismos elementos y características o los análogos de la invención.

DESCRIPCION DETALLADA DE LAS PUESTAS EN PRÁCTICA PREFERIDAS

Se hará referencia ahora en detalle a las puestas en práctica actualmente preferidas de la invención, uno o más ejemplos de los cuales están ilustrados en los dibujos acompañantes. Cada ejemplo está provisto por la vía de la explicación de la invención, no la limitación de la invención. Efectivamente, será evidente para aquellas personas experimentadas en el arte que las modificaciones y las

variaciones pueden ser hechas, en la presente invención, sin hacer abandono del alcance y del espíritu de ella. Por ejemplo, las características ilustradas o descritas como parte de una puesta en práctica, pueden ser usadas en una otra puesta en práctica, para entregar una aún otra puesta en práctica. Por consiguiente, está previsto que la presente invención cubre tales modificaciones y variaciones como viniendo dentro del alcance de las reivindicaciones anexadas y sus equivalentes.

Como es usado aquí, "datos del titular de la tarjeta de pago" se refiere a la información asociada con un titular de la tarjeta de pago, incluyendo un número de cuenta primaria (PAN) u otro número de cuenta, el nombre del titular de la tarjeta, un código de servicio y la fecha de vencimiento de la tarjeta. "Datos no sensibles del titular de la tarjeta" se refiere a los datos asociados con los dispositivos de pago procesados *in situ*, o en una red de minoristas privada, tal como los datos de las tarjetas de cliente y de programa específico. Debido a que los datos recibidos en dispositivo de entrada son inmediatamente encriptados como descrito más adelante, el sistema puede no ser capaz de distinguir entre los datos del titular de la tarjeta de pago y los datos no sensibles del titular de la tarjeta, hasta que los datos son evaluados en el sistema de evaluación segura (SEA). Por consiguiente, como es usado aquí, "datos del titular de la tarjeta" se refiere a cualquiera o ambos de los datos del titular de la tarjeta de pago y los datos no sensibles del titular de la tarjeta, antes de la evaluación en el SEA.

Las puestas en práctica de la presente invención proveen un sistema de pago minorista, el cual permite la encriptación de extremo a extremo (E2EE) de los datos del titular de la tarjeta de pago, mientras que permite el acceso a los datos no sensibles del titular de la tarjeta. El sistema comprende un SEA en el cual los datos encriptados del titular de la tarjeta, de acuerdo con un primer método de encriptación y transmitidos desde un dispositivo de entrada, puede ser evaluado de forma segura. En algunas puestas en práctica, el SEA puede comprender un candado electrónico que tiene un chip contra manipulación indebida. Si el SEA determina que los datos encriptados del titular de la tarjeta, transmitidos desde un dispositivo de entrada, son los datos no sensibles del titular de la tarjeta, los datos pueden ser hechos disponibles en forma de texto claro para el procesamiento local. Si el SEA determina que los datos encriptados del titular de la tarjeta son los datos del titular de la tarjeta de pago, los datos pueden ser encriptados de acuerdo con un segundo método de encriptación, y transmitidos a red anfitriona remota para la autenticación. Debido a que el sistema provee la encriptación de extremo a

extremo (E2EE) de los datos del titular de la tarjeta de pago, un comerciante es incapaz de acceder a los datos del titular de la tarjeta de pago en forma de texto claro. En las puestas en práctica ulteriores, un comerciante puede ser capaz de reconciliar o validar una o más transacciones a través del sistema de evaluación segura (SEA).

El término "método de encriptación", como es usado aquí, se refiere a los esquemas de encriptación, los algoritmos y/o las claves usados para encriptar y desencriptar los datos del titular de la tarjeta. El primer método de encriptación puede ser el mismo como el segundo método de encriptación, pero ellos pueden utilizar diferentes algoritmos. Debiera quedar entendido, además, que los dos métodos de encriptación pueden utilizar los mismos o similares algoritmos de encriptación, pero pueden utilizar diferentes claves de encriptación. Es decir, el primero y el segundo métodos de encriptación pueden utilizar los mismos o diferentes esquemas, estándares, algoritmos y/o claves. En muchas puestas en práctica, el primer método de encriptación puede ser provisto por el vendedor del dispositivo, encomendado con la transmisión de los datos del titular de la tarjeta al sistema de evaluación segura (SEA). Alternativamente, el primer método de encriptación es inyectado dentro del dispositivo de entrada y del SEA. El segundo método de encriptación puede ser provisto por una institución financiera, operativamente conectada con el sistema de pago minorista.

Cualquier método de encriptación adecuado, conocido por aquellas personas experimentadas en el arte, puede ser usado de acuerdo con la presente invención, pero el método usado puede preferiblemente satisfacer o bien exceder los estándares industriales. Por ejemplo, los métodos de encriptación pueden incluir Rivest-Shamir-Adelman (RSA) y triple estándar de encriptación de datos (DES). También, como apreciarán aquellas personas experimentadas en el arte, el método de encriptación usado puede ser dictaminado por los métodos de encriptación requeridos por una red anfitriona. La información de los antecedentes sobre la encriptación en los entornos minoristas está provista en la Patente de EE.UU. de N.A., N° 5.448.638 (titulada "Security Apparatus and System for Retail Environments" (*Aparato de seguridad y sistema para los entornos minoristas*), incorporada aquí como referencia en su totalidad para todos los propósitos.

Finalmente, como es usado aquí, el término "dispositivo de entrada" ampliamente se refiere a los dispositivos de seguridad, capaces de la recepción de datos del titular de la tarjeta de pago y los datos no sensibles del titular de la tarjeta, incluyendo pero no limitado a, la encriptación de teclados de PIN, teclados numéricos, pantallas táctiles, lectores de tarjeta seguros y lectores de tarjeta inteligentes. Deseablemente, todos los dispositivos de entrada usados de acuerdo con la presente invención, comprenden un procesador de encriptación seguro y una unidad de memoria o de almacenamiento. La memoria de los dispositivos de entrada almacena uno o más algoritmos de encriptación, claves y/o cifras usados para inmediatamente encriptar los datos del titular de la tarjeta después de la recepción, de acuerdo con el primer método de encriptación. En una puesta en práctica preferida, los dispositivos de entrada pueden permitir la encriptación triple DES de la clave única derivada por transacción (DUKPT) de los datos del titular de la tarjeta.

Los dispositivos de entrada también son configurados, preferiblemente, para estar contra manipulación indebida, de manera que en el caso de acceso no autorizado, los contenidos de los dispositivos de entrada, incluyendo los datos contenidos en o manipulados por el procesador del dispositivo de entrada, son borrados, cancelados o destruidos. Alternativamente, cualquier porción de los contenidos del dispositivo de entrada, suficiente para identificar los datos del titular de la tarjeta de pago, es borrada en el caso que el dispositivo de entrada está manipulado indebidamente. Sin embargo, aquellas personas experimentadas en el arte apreciarán que, en algunas puestas en práctica, donde un dispositivo de entrada está adaptado para encriptar los datos del titular de la tarjeta, tal como a través de un cabezal encriptador, el dispositivo de entrada puede no necesitar de estar contra manipulación indebida. También, en las puestas en práctica preferidas, los dispositivos de entrada pueden estar adaptados para prevenir el "*skimming*" (clonación) en tiempo real o el robo de los datos del titular de la tarjeta.

Algunas puestas en práctica de la presente invención son particularmente adecuadas para usar en las transacciones en un entorno minorista de estaciones de servicio, y la discusión más adelante describirá las puestas en práctica preferidas en ese contexto. Sin embargo, aquellas personas experimentadas en el arte entenderán que la presente invención no está limitada de ese modo.

Efectivamente, está contemplado que la presente invención sea usada con cualquier entorno minorista apropiado.

Con referencia ahora a la Figura 1, un entorno 10 de carga de combustible ejemplar puede comprender un edificio central 12, un lavado 14 de vehículos y una pluralidad de islas 16 de carga de combustible. El edificio central 12 no necesita estar centralmente ubicado dentro del entorno 10 de carga de combustible, pero por el contrario es el centro del entorno 10 de carga de combustible, y puede alojar una tienda 18 de conveniencia y/o a restaurante 20 de servicio rápido en él. Ambos, la tienda 18 de conveniencia y el restaurante 20 de servicio rápido pueden incluir un punto de venta (POS) 22, 24, respectivamente. Los POS 22, 24 pueden comprender un computador o un servidor individualmente, operativamente conectado con un lector de tarjetas asociado y un terminal de pago. Adicionalmente, los puntos de venta POS 22, 24 pueden incluir un visualizador, una pantalla táctil y/u otros dispositivos de entrada.

El edificio central 12 puede alojar, además, un controlador 26 de sitio (SC), el cual en una puesta en práctica ejemplar puede ser el sistema PASSPORT® POS, vendido por Gilbarco Inc. de Greensboro, N.C., EE.UU. de N.A., aunque pueden ser usados los controladores de sitios de terceros. El controlador 26 de sitio puede controlar la autorización de las transacciones de carga de combustible y otras actividades convencionales como está bien entendido, y el controlador 26 de sitio puede estar, preferiblemente, en comunicación operativa con cada POS. Alternativamente, el controlador 26 de sitio puede ser incorporado dentro de un POS, tal como el punto de venta 22 si es necesario o deseado.

Además, el controlador 26 de sitio puede tener un enlace 28 de comunicación *ex-situ*, permitiendo la comunicación con un sistema procesador 30 anfitrión remoto para la autorización de la tarjeta de crédito/de débito, conteniendo provisión, propósitos de reporte o los similares, cuando es necesario o deseado. En una puesta en práctica, el enlace 28 de comunicación puede ser un enrutador individual, un interruptor o una pasarela, aunque debiera ser apreciado que el controlador 26 de sitio puede realizar, adicionalmente, las funciones de, y reemplazar por ende tal un dispositivo. El enlace 28 de comunicación *ex-situ* puede ser enrutado a través de la Public Switched Telephone Network (PSTN) (*Red telefónica pública conmutada*), la Internet, ambas, o los similares, cuando es

necesario o deseado. El sistema procesador 30 anfitrión remoto puede comprender al menos un servidor mantenido por terceras partes, tal como una institución financiera. Aunque solamente un sistema procesador 30 anfitrión remoto está ilustrado, aquellas personas experimentadas en el arte apreciarán que en un sistema de pago minorista, permitiendo el pago a través de los dispositivos de pago, suministrados por múltiples compañías de tarjetas de pago o por instituciones financieras, el controlador 26 de sitio puede estar en comunicación con una pluralidad de sistemas procesadores 30 anfitriones remotos.

El lavado 14 de vehículos puede tener un punto de venta POS 32, asociado con él, que está en comunicación con el controlador 26 de sitio, para el inventario y/o los propósitos de las ventas. El lavado 14 de vehículos, alternativamente, puede ser una unidad individual. Nótese que el lavado 14 de vehículos, la tienda 18 de conveniencia y el restaurante 20 de servicio rápido son todos opcionales y no necesitan estar presentes en un entorno de carga de combustible dado.

Las islas 16 de carga de combustible pueden tener uno o más un surtidores 34 de combustible ubicados sobre ellas. Los surtidores 34 de combustible pueden ser, por ejemplo, el ENCORE® vendido por Gilbarco Inc. de Greensboro, N.C., EE.UU. de N.A. Los surtidores 34 de combustible están en comunicación electrónica con el controlador 26 de sitio, a través de cualquier enlace adecuado, tal como línea bifilar, RS 422, Ethernet, inalámbrico, etc., si es necesario o deseado.

El entorno 10 de carga de combustible también tiene uno o más tanques 36 de almacenamiento subterráneo (USTs) adaptado para mantener combustible dentro de ellos. Como tal, Los USTs 36 pueden ser cada uno un tanque de pared doble. Además, cada UST 36 puede incluir un monitor 38 de tanque (TM) asociado con él. Los monitores 38 de tanque pueden comunicarse con los surtidores 34 de combustible (ya sea a través del controlador 26 de sitio o directamente, cuando es necesario o deseado), con el fin de determinar la cantidad de combustible entregado y comparar el combustible entregado con los niveles actuales de combustible dentro de los USTs 36, con el fin de determinar si los USTs 36 tienen una fuga.

El monitor 38 de tanque puede comunicarse con el controlador 26 de sitio y puede tener, además, un enlace 40 de comunicación *ex-situ* para el reporte de la detección de fugas, reporte del inventario o los similares. Parecido como el enlace 28 de comunicación *ex-situ*, el enlace 40 de comunicación *ex-situ* puede ser a través de la PSTN, la Internet, ambas o los similares. Si el enlace 28 de comunicación *ex-situ* está presente, el enlace 40 de comunicación *ex-situ* no necesita estar presente y vice versa, aunque ambos enlaces pueden estar presentes si es necesario o deseado.

Otra información sobre y los ejemplos de los surtidores de combustible y los entornos de carga de combustible minoristas están provistos en la Patente de EE.UU. de N.A., N° 6.453.204 (titulada "Fuel Dispensing System"); 5.956.259 (titulada "Intelligent Fueling"); 5.734.851 (titulada "Multimedia Video/Graphics in Fuel Dispensers"); 6.052.629 (titulada "Internet Capable Browser Dispenser Architecture"); 5.689.071 (titulada "Wide Range, High Accuracy Flow Meter"); 6.935.191 (titulada "Fuel Dispenser Fuel Flow Meter Device, System and Method"); y 7.289.877 (titulada "Fuel Dispensing System for Cash Customers"), todas de las cuales son incorporadas aquí como referencia en sus totalidades para todos los propósitos. Un monitor 38 de tanque ejemplar puede ser el TLS-350R fabricado y vendido por la Veeder-Root Company de Simsbury, CT., EE.UU. de N.A. Para mayor información sobre los monitores de tanque y su operación, se ha hecho referencia a Patente de EE.UU. de N.A. N° 5.423.457 (titulada "Real time tank product loss detection system"); 5.400.253 (titulada "Automated Statistical Inventory Reconciliation System for Convenience Stores and Auto/truck Service Stations"); 5,319,545 (titulada "System to Monitor Multiple Fuel Dispensers and Fuel Supply Tank"); y 4.977.528 (titulada "Apparatus and Method for Determining the Amount of Material in A Tank"), todas de las cuales son incorporadas aquí como referencia en sus totalidades para todos los propósitos.

La Figura 2 ilustra un surtidor 34 de combustible que puede operar en asociación con el controlador 26 de sitio, de acuerdo con una puesta en práctica de la presente invención. El surtidor 34 incluye un sistema 42 de control, el cual puede ser un procesador, microprocesador, controlador, microcontrolador u otra electrónica adecuada, con memoria asociada y programas de soporte lógico marchando sobre ellos. En una puesta en práctica preferida, el sistema 42 de control es comparable con los sistemas de control basados en microprocesador,

usados en las unidades tipo CRIND (card reader in dispenser) (*lector de tarjeta en surtidor*) y TRIND (tag or transponder reader in dispenser) (*lector de tag o transponder en surtidor*), vendidos por Gilbarco Inc. El sistema 42 de control está en comunicación operativa con el controlador 26 de sitio. El sistema 42 de control controla, además, varios aspectos del surtidor 34 de combustible como está descrito detalladamente más adelante.

La memoria del sistema 42 de control puede ser cualquier memoria o soporte legible por computador, siempre que sea capaz de ser accedida por el sistema de control, incluyendo la memoria de acceso aleatorio (RAM), la memoria solo lectura (ROM), ROM programable y borrable (EPROM) o EPROM eléctricamente (EEPROM), CD-ROM, DVD u otro almacenamiento de disco óptico, unidad de disco estacionaria (SSD), el almacenamiento en disco magnético, incluyendo unidad de disco flexible y unidad de disco fijo, cualquier tipo de memorias no volátiles, tal como digital segura (SD), memoria instantánea, barra de memoria o cualquier otro medio que puede ser usado para portar o para almacenar código de programa de computador en la forma de programas, instrucciones o datos ejecutables por computador. El sistema 42 de control también puede incluir una porción de la memoria solamente accesible por sistema 42 de control.

En una puesta en práctica ilustrada, el surtidor 34 tiene una base 44 y una parte superior 46, con un toldo 48 soportado por dos paneles laterales 50. El surtidor 34 de combustible está subdividido en múltiples compartimentos. Un área hidráulica 52 abarca los componentes hidráulicos y un área electrónica 54 encierra los componentes electrónicos. Una barrera de vapor puede ser usada para separar el área hidráulica 52 del área electrónica 54.

Varios componentes usados para el control del caudal de combustible pueden ser alojados dentro del área hidráulica 52. El combustible proveniente de los USTs 36 es bombeado a través de una red de tuberías dentro de la tubería 56 de entrada. El combustible que está siendo entregado pasa a través de un medidor 58, el cual responde respecto al caudal o volumen. Un sensor 60 de desplazamiento es empleado para generar una señal en respuesta al caudal de combustible a través del medidor 58. Las líneas 62 de control/de datos proveen una vía de señalización desde el sensor 60 hacia el sistema 42 de control, y

proporciona señales hacia el sistema 42 de control indicativas sobre el caudal de combustible que está siendo entregado. Las líneas 62 de control/de datos pueden proveer señalización de control hacia una válvula 64, que puede ser abierta y cerrada con el fin de permitir o no permitir la entrega de combustible.

Las mediciones del caudalímetro desde el sensor 60 son recolectadas por el sistema 42 de control. El sistema 42 de control también realiza, típicamente, los cálculos tal como el costo asociado con una transacción de expendio de combustible. Adicionalmente, el sistema 42 de control controla el procesamiento transaccional en un surtidor 34 de combustible como será descrito detalladamente más adelante.

Cuando progresa una transacción de expendio, el combustible es entregado entonces a una manguera 66 y, a través de una tobera 68 dentro del vehículo del cliente. El surtidor 34 incluye una funda 70 de tobera, la cual puede ser usada para sujetar y retener la tobera 68 cuando no está en uso. La funda 70 de tobera puede incluir un interruptor mecánico o eléctrico, para indicar cuando la tobera 68 ha sido removida para el requerimiento de expendio de combustible, y cuando la tobera 68 ha sido reubicada, significando el término de la transacción de carga de combustible. Una línea de control provee una vía de señalización desde el interruptor de la electrónica hacia el sistema 42 de control. El sistema 42 de control puede usar la señalización recibida a través de la línea de control, con el fin de hacer una determinación sobre cuándo una transacción ha sido iniciada o completada.

Las líneas 72 de control/de datos proveen comunicación electrónica entre el sistema 42 de control y una interfaz 74 de usuario. La interfaz 74 de usuario incluye varias combinaciones de subsistemas para facilitar la interacción del cliente con el surtidor 34 y la aceptación del pago por el combustible entregado. Un bisel 76 actúa como un labio alrededor de varios subsistemas de la interfaz 74. En la mayoría de los casos, el bisel 76 está enrasado con la cara del surtidor de combustible; sin embargo, en algunas puestas en práctica puede extenderse hacia fuera desde la cara, en efecto formando un labio en resalte. El bisel 76 también puede comprender una pluralidad de secciones que enmarca o aloja varios subsistemas o componentes.

Como se muestra, la interfaz 74 de usuario incluye diversos dispositivos de entrada. Por ejemplo, la interfaz 74 de usuario puede incluir teclado numérico 78. El teclado numérico 78 es usado, típicamente, para la entrada de un PIN si el cliente está usando una tarjeta de débito para el pago de combustible u otros bienes o servicios. En una puesta en práctica preferida, el teclado numérico 78 puede ser el teclado de PIN encriptador FlexPay™ ofrecido por Gilbarco Inc.

La interfaz 74 de usuario también puede incluir un lector 80 de tarjeta seguro para la aceptación de las tarjetas de crédito, de débito u otras de banda magnética para el pago. Adicionalmente, el lector 80 de tarjeta seguro puede aceptar las tarjetas de cliente o de programa específico como descrito anteriormente. El lector 80 de tarjeta comprende un mecanismo para la recepción de los datos de tarjeta de pago, tal como un cabezal lector en el caso de un lector de tarjetas de banda magnética, así como también al menos un puerto de entrada-salida ("I/O") para la recepción de y la carga de las claves de encriptación del primer método de encriptación. En las puestas en práctica preferidas actualmente, el lector 80 de tarjeta puede ser análogo con el lector de tarjetas seguro MagTek® PermaSeal o el lector de tarjetas seguro FlexPay™ ofrecido por Gilbarco Inc.

La interfaz 74 de usuario también puede incluir otros dispositivos de entrada, tal como un lector 82 de tarjetas sin contacto (por ejemplo, para circuitos integrados o tarjetas "inteligentes"). Además, el interfaz 74 de usuario puede incluir otros dispositivos de pago y transaccionales tal como un aceptador 84 de billetes, un impresor 86 de recibos y un dispositivo 88 para entrega de cambio. El impresor 86 de recibos puede proveer a un cliente con recibo con un registro de la transacción llevada a cabo en un surtidor 34 de combustible. El dispositivo 88 para entrega de cambio puede entregar el cambio a un cliente por el sobrepago. Otros dispositivos transaccionales, tal como un lector óptico y un lector biométrico, también están contemplados.

Un visualizador 90 puede ser usado para visualizar la información, tal como las peticiones y la publicidad relacionadas con la transacción, al cliente. En algunas puestas en práctica, una pantalla táctil puede ser usada por el visualizador 90. En este caso, el visualizador 90 puede ser configurado para visualizar un teclado numérico virtual, para la recepción de los datos de pago, tal como un PIN de una tarjeta de débito o el código postal de facturación de una

tarjeta de crédito, por ejemplo. El visualizador 90 también puede ser usado para recibir una selección desde el cliente observando la información visualizada.

El cliente puede usar las teclas programables 92 para responder a los requerimientos de información presentados al usuario, a través del visualizador 90. Un intercomunicador 94 puede ser provisto para generar indicadores audibles para el cliente, y para permitir al cliente de interactuar con un dependiente. En adición, el surtidor 34 puede incluir un visualizador 96 del total del precio de la transacción, que presenta al cliente con el precio para el combustible que ha sido entregado. Un visualizador 96 del total de galones de la transacción puede ser usado para presentar al cliente con la medición del combustible en las unidades de galones o litros. Los botones 100 de selección de octanos pueden ser provistos para que el cliente seleccione cual grado de combustible ha de ser entregado antes del inicio del expendio. Finalmente, los visualizadores 102 de precio por unidad (PPU) pueden ser provistos para mostrar el precio por unidad del combustible entregado en ya sea galones o litros, dependiendo de la programación del surtidor 34.

La Figura 3 provee una ilustración diagramática de un sistema de pago teniendo un sistema de evaluación seguro (SEA), de acuerdo con una puesta en práctica de la presente invención. En general, el SEA permite un sistema de pago minorista para proveer la encriptación de extremo a extremo (E2EE) de los datos del titular de la tarjeta de pago, mientras que permite el acceso a los datos no sensibles del titular de la tarjeta para el procesamiento local. Más particularmente, como explicado anteriormente en referencia a las Figuras 1 y 2, los surtidores 34 de combustible pueden comprender una interfaz de usuario comprendiendo uno o más dispositivos de entrada 104, tal como un lector de tarjetas seguro. Los dispositivos 104 de entrada están en comunicación electrónica con el sistema 42 de control, y el sistema 42 de control está en comunicación operativa con el controlador 26 de sitio. También, el punto de venta POS 22 (ó 24, 32) comprende uno o más dispositivos de entrada 104, y está en comunicación operativa con el controlador 26 de sitio. El controlador 26 de sitio puede estar en comunicación con N sistemas procesadores 30 anfitriones remotos a través del enlace 28 de comunicación *ex-situ*. Aunque solamente un POS 22 y un surtidor 34 de combustible son mostrados en la Figura 3 para facilitar la ilustración, aquellas personas experimentadas en el arte apreciarán que el controlador 26 de sitio

puede, típicamente, comunicar con una pluralidad de POS 22 y de los surtidores 34 de combustible.

De acuerdo con las puestas en práctica de la presente invención, cualquier dispositivo en el sistema de pago minorista, el cual manipula o procesa los datos del titular de la tarjeta, puede comprender un SEA (en adelante un "dispositivo de manipulación de los datos del titular de la tarjeta"), incluyendo los dispositivos de entrada descritos anteriormente. Como descrito detalladamente más adelante, un SEA comprende, preferiblemente, la electrónica de control respecto a la manipulación indebida y memoria encriptada. El SEA puede ser adaptado para recibir los datos encriptados del titular de la tarjeta desde uno o más dispositivos de entrada, y evalúa los datos dentro la electrónica de control respecto a la manipulación indebida, con el fin de determinar si son los datos del titular de la tarjeta de pago, o los datos no sensibles del titular de la tarjeta. El SEA también puede comprender un registro de transacción encriptada, contra el cual los datos encriptados del titular de la tarjeta de pago pueden ser comparados para los propósitos de reconciliación o de validación.

Como se muestra, por ejemplo, un sistema 106 de evaluación segura (SEA) puede estar operativamente conectado con cualquiera del controlador 26 de sitio, POS 22, y un surtidor de combustible sistema 42 de control. El controlador 26 de sitio y el POS 22 son mostrados como dispositivos separados en la Figura 3, pero será apreciado que el controlador 26 de sitio puede ser incorporado dentro de un POS 22 como indicado anteriormente. En una puesta en práctica preferida, el SEA puede comprender un candado electrónico, que puede ser acoplado a un dispositivo de manipulación de los datos del titular de la tarjeta. Por ejemplo, el SEA 106 puede tener una interfaz de bus serial universal (USB) que puede ser conectada a un puerto USB en el POS 22. Alternativamente, el candado electrónico puede estar ubicado dentro de un surtidor 34 de combustible y conectado a una interfaz USB en el sistema 42 de control. Aunque el SEA pueda comunicarse con un dispositivo de manipulación de los datos del titular de la tarjeta, a través de cualquier interfaz adecuada, incluyendo pero no limitado a Ethernet e interfaces seriales y paralelas, aquellas personas experimentadas en el arte apreciarán que la velocidad alta de las comunicaciones que ofrece una interfaz USB, puede ser deseable para ciertas funciones del SEA, incluyendo la reconciliación. Además, donde el SEA está implementado como un candado

electrónico, el SEA puede ser movido fácilmente desde un dispositivo de manipulación de los datos del titular de la tarjeta hacia otro, en caso del malfuncionamiento del primer dispositivo.

De acuerdo con una alternativa puesta en práctica, el SEA puede ser implementado como una unidad de procesamiento central (CPU) contra manipulación indebida en lugar de un candado electrónico. Como con la puesta en práctica del candado electrónico, la CPU puede ser provista en cualquier dispositivo de manipulación de los datos del titular de la tarjeta. En algunos casos, la CPU puede reubicar y realizar las funciones del procesador o sistema de control del dispositivo. La CPU puede comprender una memoria encriptada que puede ser análoga con la memoria SEA encriptada descrita más adelante. Esta memoria encriptada puede ser en adición a otra memoria interna de la CPU. En la alternativa, la CPU pueden comunicarse con una memoria SEA encriptada externa a la CPU. En una puesta en práctica, the la CPU contra manipulación indebida puede ser análoga con el controlador seguro descrito en la Publicación antes de Concesión de EE. UU. de N.A. N° 2009/0265638, titulada "System y Method for Controlling Secure Content and Non-secure Content at a Fuel Dispenser o Other Retail Device," incorporada aquí como referencia en su totalidad para todos los propósitos.

Aunque las puestas en práctica están contempladas en la cual más que una SEA 106 está provista, un sistema de pago minorista, de acuerdo con la presente invención puede comprender, preferiblemente, un SEA 106 individual el cual recibe y evalúa todos los datos encriptados del titular de la tarjeta, transmitidos a través del sistema. En otras palabras, el SEA 106 puede evaluar los datos encriptados del titular de la tarjeta, transmitidos mediante un dispositivo 104 de entrada a pesar de la ubicación del SEA 106 y del dispositivo 104 de entrada. Por ejemplo, si el POS 22 comprende un SEA 106 y un cliente provee los datos del titular de la tarjeta, a través de un dispositivo 104 de entrada en un surtidor 34 de combustible, los datos encriptados del titular de la tarjeta son todavía transmitidos al SEA 106 para la evaluación. Aquellas personas experimentadas en el arte apreciarán que esto puede facilitar la conformidad con los estándares industriales.

La Figura 4 es una ilustración esquemática de un SEA adaptado para la evaluación de forma segura los datos del titular de la tarjeta, transmitidos desde un

dispositivo de entrada hacia un sistema procesador anfitrión remoto, de acuerdo con una puesta en práctica de la presente invención. En particular, el dispositivo 104 de entrada, el cual comprende un procesador 108 de encriptación seguro y una memoria 110, puede estar en comunicación electrónica con el SEA 106. El procesador 108 puede ser adaptado para inmediatamente encriptar los datos del titular de la tarjeta, recibidos en el dispositivo 104 de entrada de acuerdo con el primer método de encriptación, basado en la encriptación de las claves ubicadas en la memoria 110. El SEA 106 también puede estar en comunicación electrónica con el sistema procesador 30 anfitrión remoto. Las comunicaciones encriptadas entre el dispositivo 104 de entrada y el SEA 106, y entre el SEA 106 y el sistema procesador 30 anfitrión remoto, pueden pasar a través de uno o más dispositivos intermediarios, dependiendo de las respectivas ubicaciones del dispositivo 104 de entrada y del SEA 106 dentro el sistema de pago minorista. Finalmente, el SEA 106 está preferiblemente en comunicación electrónica con un sistema 112 de procesamiento local, el cual puede comprender uno o más dispositivos en comunicación con una red minorista local o privada, adaptada para recibir y procesar los datos no sensibles del titular de la tarjeta. Esto puede ocurrir, por ejemplo, en el sistema punto de venta (POS) dentro del entorno de carga de combustible.

El SEA comprende, preferiblemente, la memoria SEA encriptada y la electrónica de control contra manipulación indebida. La electrónica de control respecto a la manipulación indebida también puede comprender la memoria interna. Estas memorias pueden comprender instrucciones o códigos de programa ejecutables en computador que, cuando son ejecutados por la electrónica de control contra manipulación indebida, realizan uno o más pasos de los procesos descritos anteriormente y detalladamente más adelante. Las memorias también pueden comprender los datos y una o más estructuras de datos para el almacenamiento de información. Las instrucciones o códigos de programas ejecutados por computadora en este escenario, como debiera ser conocido por aquellas personas experimentadas en el arte, usualmente incluyen uno o más programas de aplicación, otros módulos de programa, datos de programa, firmware y/o un sistema operativo.

Como se muestra, por ejemplo, el SEA 106 comprende una memoria 114 del SEA y la electrónica 116 de control respecto a la manipulación indebida

teniendo una memoria interna 118. Un suministro 120 de energía, tal como una batería o los similares, puede ser provisto para preservar la integridad de los datos en la memoria 118 y energizar la electrónica 116 de control respecto a la manipulación indebida, cuando el SEA 106 no está conectado a una fuente de energía primaria, tal como un dispositivo de manipulación de los datos del titular de la tarjeta. Las comunicaciones hacia y desde el SEA 106 pueden pasar a través de una interfaz USB 122, como discutido anteriormente.

La electrónica de control respecto a la manipulación indebida puede estar, preferiblemente, implementada como un circuito integrado seguro (IC) o chip. Además, la electrónica de control respecto a la manipulación indebida incorpora, preferiblemente, los mecanismos de protección físicos y/o lógicos diseñados para impedir la manipulación indebida. En una puesta en práctica actualmente preferida, la electrónica 116 de control respecto a la manipulación indebida puede ser la USIP™ Professional IC, vendida por Maxim Integrated Products, Inc. of Sunnyvale, CA, EE.UU. de N.A. Sin embargo, aquellas personas experimentadas en el arte apreciarán que cualquier electrónica de control proveyendo funcionalidad análoga puede ser usada por electrónica de control 116. De forma importante, la electrónica de control respecto a la manipulación indebida está programada, preferiblemente, para denegar la pasada de los datos del titular de la tarjeta de pago desde el SEA, a menos que esté encriptada de acuerdo con el segundo método de encriptación.

La memoria interna de la electrónica de control respecto a la manipulación indebida puede comprender cualquier tipo de memoria, como discutido anteriormente en referencia al sistema 42 de control y puede almacenar, preferiblemente, uno o más algoritmos de encriptación, claves y/o cifras usadas para comunicar con la memoria SEA encriptada, de acuerdo con un tercer método de encriptación. En una puesta en práctica, la memoria interna 118 puede comprender una memoria estática de acceso aleatorio (SRAM). También, en el caso de acceso no autorizado, los mecanismos de protección descritos anteriormente están habilitados, preferiblemente, para borrar, cancelar o destruir los contenidos en la memoria interna. Por consiguiente, por ejemplo, si un ladrón intenta de obtener las claves de desencriptación para el tercer método de encriptación desde la memoria 118 mediante la manipulación indebida con la electrónica 116 de control respecto a la manipulación indebida, los mecanismos de

protección pueden causar que las claves de descryptación para el tercer método de encriptación (o la totalidad de la memoria 118) sean borradas. En cualquier caso, la memoria 114 del SEA encriptada ya no sería legible. Además, la memoria interna de la electrónica de control respecto a la manipulación indebida puede incluir una máquina procesadora de tarjetas. En particular, la máquina procesadora de tarjetas puede evaluar los datos del titular de la tarjeta, que han sido no encriptados dentro de la electrónica de control respecto a la manipulación indebida, con el fin de determinar si los datos del titular de la tarjeta debieran ser encriptados, de acuerdo con el segundo método de encriptación, y transmitidos a un sistema procesador anfitrión remoto o hacerlos disponibles en forma de texto claro para el procesamiento local.

Como indicado anteriormente, la memoria 114 del SEA puede ser encriptada de acuerdo con un tercer método de encriptación. Preferiblemente, la electrónica de control respecto a la manipulación indebida puede emplear encriptación sobre la marcha (OTFE) para leer desde y escribir hacia la memoria del SEA encriptada. El tercer método de encriptación es, preferiblemente, distinto con respecto al primero y segundo métodos de encriptación, y en una puesta en práctica, el tercer método de encriptación puede ser el 128-bit Advanced Encryption Standard (AES-128) (*Estándar de encriptación avanzada de 128 bit*). Deseablemente, el chip USIP™ puede realizar la OTFE de una memoria del SEA usando AES-128.

En las puestas en práctica preferidas, la memoria 114 del SEA puede estar, preferiblemente, inyectadas con las claves de descryptación para el primer método de encriptación, y las claves de encriptación para el segundo método de encriptación. De ese modo, la electrónica 116 de control respecto a la manipulación indebida puede descryptar los datos del titular de la tarjeta, transmitidos hacia el SEA 106 desde un dispositivo de entrada, y encriptar los datos del titular de la tarjeta de pago antes de transmitirlos hacia un sistema procesador anfitrión remoto. La memoria 114 del SEA puede comprender, preferiblemente, una memoria instantánea, pero como con la memoria interna de la electrónica de control respecto a la manipulación indebida, discutida anteriormente, la memoria del SEA puede comprender cualquier tipo adecuado de memoria. También, como está descrito detalladamente más adelante, la memoria 114 del SEA encriptada almacena, preferiblemente, un archivo de configuración

del sitio contra el cual los datos del titular de la tarjeta pueden ser comparados y un archivo de registro par los propósitos de reconciliación o de validación.

La Figura 5 es un diagrama de flujo ilustrando un método ejemplar para el procesamiento de una transacción, involucrando los datos del titular de la tarjeta usando el sistema de la Figura 4. El proceso arranca (paso 200) y un usuario inicia una transacción en el dispositivo 104 de entrada. El dispositivo 104 de entrada recibe los datos del titular de la tarjeta desde el dispositivo de pago del usuario (paso 202), inmediatamente encripta los datos del titular de la tarjeta, de acuerdo con el primer método de encriptación (paso 204), y transmite los datos encriptados del titular de la tarjeta hacia el SEA 106. Los datos encriptados del titular de la tarjeta transmitidos desde el dispositivo 104 de entrada, son recibidos en la electrónica 116 de control respecto a la manipulación indebida en el SEA 106 (paso 206).

Como discutido anteriormente, la electrónica 116 de control respecto a la manipulación indebida puede emplear, preferiblemente, la encriptación sobre la marcha (OTFE) cuando accede a la memoria 114 del SEA. Por consiguiente, la memoria 114 del SEA y/o los datos relevantes almacenados sobre ella pueden ser no encriptados automáticamente, y encriptados usando las claves del tercer método de encriptación, cada vez que la electrónica 116 de control con respecto a la manipulación indebida lea desde o escribe hacia la memoria 114 del SEA.

A continuación, la electrónica 116 de control con respecto a la manipulación indebida puede acceder a un archivo de configuración del sitio almacenado en la memoria 114 (paso 208). Además, usando las claves de desencriptación del primer método de encriptación, la electrónica 116 de control con respecto a la manipulación indebida, puede desencriptar los datos del titular de la tarjeta (paso 210). El archivo de configuración del sitio contiene, preferiblemente, los criterios que la electrónica 116 de control respecto a la manipulación indebida, puede usar con el fin de determinar si los datos del titular de la tarjeta son los datos del titular de la tarjeta de pago, o los datos no sensibles del titular de la tarjeta. Donde un dispositivo de entrada está adaptado para recibir los datos del titular de la tarjeta de pago, emitidos por más que una institución financiera, el archivo de configuración del sitio también puede contener una tabla de consulta asociando una porción de los datos del titular de la tarjeta de pago, tal como los primeros seis

dígitos del número de cuenta primaria (PAN), con una institución financiera particular.

A continuación, la electrónica 116 de control respecto a la manipulación indebida puede comparar los datos del titular de la tarjeta, con respecto el archivo de configuración del sitio, almacenado en la memoria 114, con el fin de determinar si los datos del titular de la tarjeta son los datos del titular de la tarjeta de pago, o los datos no sensibles del titular de la tarjeta (paso 212). Si los datos son los datos del titular de la tarjeta de pago, la electrónica 116 de control respecto a la manipulación indebida, puede almacenar un registro de la transacción en un archivo de registro en la memoria 114 (paso 214). Los datos almacenados pueden incluir la cantidad total de la transacción, y al menos una porción de los datos del titular de la tarjeta de pago, tal como el PAN asociado con la cuenta del cliente. Un comerciante puede requerir esta información por varias razones, tal como para la contabilidad o los reportes.

En una puesta en práctica alternativa, discutida detalladamente más adelante, la electrónica 116 de control respecto a la manipulación indebida puede almacenar, en su lugar, solamente un número de referencia de consulta de transacción en la memoria 114. El número de referencia de consulta de transacción puede ser único para cada transacción. En este caso, los detalles de la transacción pueden ser almacenados en un archivo de registro en una memoria externa, tal como aquella del dispositivo de manipulación de los datos del titular de la tarjeta, o un sistema remoto, junto con el asociado número de referencia de consulta de transacción. De ese modo, los datos del titular de la tarjeta de pago pueden permanecer seguramente encriptados sin la eliminación de la capacidad del comerciante para realizar la validación de la transacción.

En cualquier caso, la electrónica 116 de control respecto a la manipulación indebida puede entonces encriptar los datos del titular de la tarjeta de pago, usando las claves de encriptación del segundo método de encriptación almacenado en la memoria 114 (paso 216). En una puesta en práctica, el mismo segundo método de encriptación es usado independientemente de la institución financiera, a la cual corresponden los datos del titular de la tarjeta de pago. En una otra puesta en práctica, el archivo de configuración del sitio en la memoria 114 es usado para identificar cual segundo método de encriptación se va a usar cuando

se encripten los datos del titular de la tarjeta de pago. En particular, la tabla de consulta en el archivo de configuración del sitio también puede contener el segundo esquema de encriptación requerido por cada institución financiera. En tal una puesta en práctica, los múltiples segundos métodos de encriptación (correspondientes a las respectivas instituciones financieras) también pueden ser almacenados dentro de la memoria 114. Una vez que la electrónica 116 de control respecto a la manipulación indebida identifica la institución financiera, asociada con los datos del titular de la tarjeta de pago, el segundo método de encriptación aplicable es seleccionado y usado para encriptar los datos del titular de la tarjeta de pago.

La electrónica 116 de control respecto a la manipulación indebida puede finalmente transmitir los datos encriptados del titular de la tarjeta de pago hacia el sistema procesador 30 anfitrión remoto (paso 218). El proceso termina entonces (paso 220). El sistema procesador 30 anfitrión remoto puede devolver un mensaje ya sea autorizando o denegando la autorización de la transacción de la tarjeta de pago. De acuerdo con una otra puesta en práctica, la electrónica de control con respecto a la manipulación indebida puede almacenar esta información en el archivo de registro en la memoria 114 del SEA encriptada.

Retornando al paso 212, si los datos del titular de la tarjeta no satisfacen los criterios de los datos del titular de la tarjeta de pago en el archivo de configuración del sitio en la memoria 114, el sistema puede determinar que los datos del titular de la tarjeta son los datos no sensibles del titular de la tarjeta. En este caso, la electrónica 116 de control respecto a la manipulación indebida puede transmitir los datos no sensibles del titular de la tarjeta, en forma de texto claro, al sistema 112 de procesamiento local (paso 222). El sistema 112 de procesamiento local puede usar los datos no sensibles del titular de la tarjeta, con el fin de proveer un crédito para una transacción o un descuento sobre el combustible, por ejemplo. Aunque no está ilustrado en esta puesta en práctica, la electrónica 116 de control respecto a la manipulación indebida también puede almacenar un registro de la transacción en el archivo de registro. El proceso termina entonces (paso 220).

Como indicado anteriormente, cualquier dispositivo de manipulación de los datos del titular de la tarjeta puede comprender un SEA, incluyendo un controlador de sitio, un punto de venta (POS) y un sistema de control del surtidor de

combustible. En algunas puestas en práctica, dependiendo de la cantidad de información almacenada, el archivo de registro de la transacción puede resultar más grande que la memoria del SEA. En este caso, la memoria (por ejemplo, un disco duro) en el dispositivo de manipulación de los datos del titular de la tarjeta, comprendiendo el SEA, puede almacenar el registro de transacción grande, nuevamente encriptados de acuerdo con el método de encriptación. Entonces, la electrónica de control respecto a la manipulación indebida del SEA puede leer desde y escribir hacia el registro en la manera descrita anteriormente. En una otra puesta en práctica, el archivo de registro de la transacción puede ser almacenado en y accedido sobre un sistema remoto, tal como un computador o servidor remotos asociados con una pluralidad de sistemas de pago al por menor. También, una copia de respaldo del registro puede ser periódicamente transmitida desde el SEA hacia el sistema remoto. Aquí, por ejemplo, el SEA puede comunicarse con el sistema remoto a través del enlace 28 de comunicación *ex-situ*, el cual en una puesta en práctica puede ser enrutado a través de la Internet.

De acuerdo con una otra puesta en práctica, la presente invención contempla un método mediante el cual un comerciante puede realizar la reconciliación o la validación de disputada transacción. En este sentido, la Figura 6 es un diagrama de flujo ilustrando un método ejemplar para el procesamiento de una solicitud con el fin de validar una transacción involucrando datos del titular de la tarjeta de pago usando el sistema de la Figura 4. The sistema de pago minorista puede comprender una interfaz de programación de aplicaciones (API), el cual permite a un comerciante de proveer los datos del titular de la tarjeta de pago desde un cliente disputando una transacción con el SEA y requerir la información considerando si la transacción es válida. Como descrito más adelante, el SEA está adaptado para responder a este requerimiento en una puesta en práctica, sin hacer disponibles los datos del titular de la tarjeta de pago en la forma de texto claro. En otras puestas en práctica, está contemplado que la API puede ser usada en una forma similar para realizar la reconciliación. La API puede ser implementada como un programa de soporte lógico sobre un computador o un servidor en comunicación operativa con el SEA, tal como en un computador o un servidor asociado con el POS 22.

El proceso arranca (paso 300), y un comerciante inicia un requerimiento de validación de la transacción a través de la API y obtiene los datos del titular de la

tarjeta de pago de un cliente a través del dispositivo 104 de entrada (paso 302). El dispositivo 104 de entrada inmediatamente encripta los datos del titular de la tarjeta de pago, de acuerdo con el primer método de encriptación (paso 304), y transmite los datos encriptados del titular de la tarjeta de pago hacia el SEA 106. Los datos encriptados del titular de la tarjeta de pago transmitidos desde dispositivo 104 de entrada, son recibidos en la electrónica 116 de control respecto a la manipulación indebida en el SEA 106 (paso 306).

A continuación, la electrónica 116 de control respecto a la manipulación indebida puede acceder a un registro de transacción almacenado en la memoria 114 (paso 308). Como descrito anteriormente, debido a que la memoria 114 está encriptada de acuerdo con el tercer método de encriptación, la electrónica 116 de control respecto a la manipulación indebida, la cual posee las claves de encriptación y desencriptación del tercer método de encriptación, puede emplear la encriptación sobre la marcha (OTFE) cuando accede a la memoria 114. Usando las claves de desencriptación del primer método de encriptación, almacenadas en la memoria 114, la electrónica 116 de control respecto a la manipulación indebida puede acceder a los datos del titular de la tarjeta de pago (paso 310).

A continuación, la electrónica 116 de control respecto a la manipulación indebida puede comparar los datos del titular de la tarjeta de pago con respecto al archivo de registro de la transacción almacenado en la memoria 114, con el fin de determinar si los datos del titular de la tarjeta de pago corresponden a una transacción procesada en el sitio del comerciante (paso 312). Si es así, la electrónica 116 de control respecto a la manipulación indebida puede proveer los detalles considerando la transacción con el comerciante, preferiblemente, omitiendo los datos del titular de la tarjeta de pago (paso 314). Los detalles pueden incluir la hora de la transacción, la cantidad cargada, o los bienes o servicios adquiridos. Por consiguiente, el comerciante puede obtener la validación de una transacción sin los datos del titular de la tarjeta de pago, que están siendo accesibles en forma de texto claro. El proceso termina en el paso 316. Sin embargo, basado en la evaluación del archivo de registro, si los datos del titular de la tarjeta de pago no corresponden a una transacción procesada en el sitio del comerciante, la electrónica de control respecto a la manipulación indebida puede entregar un mensaje apropiado, para así informar al comerciante (paso 318). El proceso nuevamente termina en el paso 316.

En una puesta en práctica alternativa, donde el registro de la transacción es almacenado en una memoria externa a la memoria 114 del SEA 106 y asociado con un número de referencia de consulta de transacción, un comerciante puede nuevamente iniciar un requerimiento de validación de la transacción, como descrito anteriormente en los pasos 300-306. En este caso, sin embargo, la electrónica 116 de control respecto a la manipulación indebida, puede acceder al número de referencia de consulta de transacción para la transacción requerida. La electrónica 116 de control con respecto a la manipulación indebida puede entonces proveer el número de referencia de consulta al comerciante. El comerciante puede usar el número de referencia de consulta para acceder a los detalles de la transacción, almacenada en un registro en una memoria externa y asociado con el número de referencia de consulta.

Basado en lo anterior, aquellas personas experimentadas en el arte apreciarán que el SEA puede proveer la encriptación de extremo a extremo (E2EE) de los datos del titular de la tarjeta de pago. De acuerdo con las puestas en práctica preferidas, los datos del titular de la tarjeta son solamente no encriptados y evaluados dentro de la electrónica de control contra manipulación indebida, y, cuando son almacenados, los datos del titular de la tarjeta de pago están almacenados en la memoria del SEA, encriptados de acuerdo con el tercer método de encriptación. La electrónica de control respecto a la manipulación indebida es, preferiblemente, el único dispositivo en el sistema de pago minorista capaz de desenscriptar la memoria del SEA. Además, la electrónica de control con respecto a la manipulación indebida puede ser programada para jamás pasar los datos encriptados del titular de la tarjeta de pago desde el SEA. Tal una disposición puede deseablemente satisfacer ciertos requerimientos de seguridad de la industria de las tarjetas de pago, o de evitar tales requerimientos completamente.

Mientras que una o más de las puestas en práctica preferidas de la invención han sido descritas anteriormente, debiera quedar entendido que cualquiera y todas las realizaciones equivalentes de la presente invención, están incluidas dentro del alcance y del espíritu de ella. Las puestas en práctica descritas están representadas solamente por la vía del ejemplo y no están previstas como limitaciones sobre la presente invención. Por consiguiente, debiera quedar entendido por aquellas personas experimentadas comunes en este arte,

que la presente invención no está limitada a estas puestas en práctica, puesto que se pueden hacer modificaciones. Por lo tanto, está contemplado que cualquiera y todas tales puestas en práctica están incluidas en la presente invención como pueden caer dentro del alcance y del espíritu de ella.

REIVINDICACIONES

1. Un sistema usado en un entorno minorista para la provisión de la encriptación de extremo a extremo de los datos del titular de la tarjeta de pago, CARACTERIZADO porque dicho sistema comprende:

un dispositivo de entrada configurado para recibir los datos del titular de la tarjeta, dicho dispositivo de entrada está operativo para encriptar dichos datos del titular de la tarjeta, de acuerdo con un primer método de encriptación, con el fin de producir los primeros datos encriptados del titular de la tarjeta;

un dispositivo de manipulación de los datos del titular de la tarjeta, en comunicación electrónica con dicho dispositivo de entrada;

un sistema de evaluación segura, operativamente conectado con dicho dispositivo de manipulación de los datos del titular de la tarjeta, comprendiendo dicho sistema de evaluación segura la electrónica de control respecto a la manipulación indebida, adaptada para desenscriptar dichos primeros datos encriptados del titular de la tarjeta, con el fin de producir los datos no encriptados del titular de la tarjeta;

donde dicha electrónica de control respecto a la manipulación indebida, de dicho sistema de evaluación segura, evalúa dichos datos no encriptados del titular de la tarjeta, con el fin de determinar si dichos datos no encriptados del titular de la tarjeta son los datos del titular de la tarjeta de pago, o los datos no sensibles del titular de la tarjeta; y

donde, si dichos datos no encriptados del titular de la tarjeta son los datos del titular de la tarjeta de pago, dicha electrónica de control respecto a la manipulación indebida de dicho sistema de evaluación segura, está adaptada para encriptar dichos datos no encriptados del titular de la tarjeta, de acuerdo con un segundo método de encriptación, con el fin de producir los segundos datos encriptados del titular de la tarjeta.

2. Un sistema como en la reivindicación 1, CARACTERIZADO porque dicho sistema de evaluación segura transmite dichos datos no encriptados del titular de la tarjeta hacia un sistema de procesamiento local, en una forma no encriptada, si dichos datos no encriptados del titular de la tarjeta son los datos no sensibles del titular de la tarjeta.

3. Un sistema como en la reivindicación 2, CARACTERIZADO porque dicho sistema de evaluación segura está implementado como a candado electrónico.
4. Un sistema como en la reivindicación 3, CARACTERIZADO porque dicho candado electrónico comprende una interfaz USB.
5. Un sistema como en la reivindicación 2, CARACTERIZADO porque dicha electrónica de control respecto a la manipulación indebida are implementada como un chip USIP.
6. Un sistema como en la reivindicación 1, CARACTERIZADO porque dicho sistema de evaluación segura está adaptado para transmitir dichos segundos datos encriptados del titular de la tarjeta hacia un sistema procesador anfitrión remoto.
7. Un sistema como en la reivindicación 1, CARACTERIZADO porque dichos primer y segundo métodos de encriptación son los mismos.
8. Un sistema como en la reivindicación 1, CARACTERIZADO porque dichos primer y segundo métodos de encriptación son diferentes.
9. Un sistema como en la reivindicación 1, CARACTERIZADO porque dicho primer método de encriptación comprende la encriptación triple DES de los datos del titular de la tarjeta.
10. Un sistema como en la reivindicación 9, CARACTERIZADO porque dicho dispositivo de entrada es contra la manipulación indebida.
11. Un sistema como en la reivindicación 1, CARACTERIZADO porque dicho dispositivo de manipulación de los datos del titular de la tarjeta, es seleccionado entre el grupo que consta de un sistema de control del surtidor de combustible, un POS y un controlador de sitio.
12. Un sistema de evaluación segura, en el cual una comunicación encriptada de los datos del titular de la tarjeta, desde un dispositivo de entrada hacia

un sistema procesador anfitrión remoto, puede ser evaluada de forma segura, CARACTERIZADO porque comprende:

una electrónica de control seguro; y

una memoria del sistema de evaluación segura, conteniendo dicha memoria del sistema de evaluación segura la información necesitada para descryptar los datos encriptados, de acuerdo con un primer método de encriptación, y la información necesitada para encriptar los datos de acuerdo con un segundo método de encriptación;

siendo dicha memoria del sistema de evaluación segura encriptada de acuerdo con un tercer método de encriptación;

donde dicha electrónica de control seguro está adaptada para descryptar dicha memoria del sistema de evaluación segura;

donde dicha electrónica de control seguro está adaptada ulteriormente para descryptar los datos encriptados del titular de la tarjeta, de acuerdo con dicho primer método de encriptación, con el fin de producir los datos no encriptados del titular de la tarjeta;

donde dicha electrónica de control seguro está adaptada ulteriormente para evaluar dichos datos no encriptados del titular de la tarjeta, y encriptar dichos datos no encriptados del titular de la tarjeta, de acuerdo con dicho segundo método de encriptación, si dichos datos no encriptados del titular de la tarjeta son los datos del titular de la tarjeta de pago.

13. Un sistema de evaluación segura como en la reivindicación 12, CARACTERIZADO porque dichos primer y segundo métodos de encriptación son diferentes.
14. Un sistema de evaluación segura como en la reivindicación 13, CARACTERIZADO porque dicha memoria del sistema de evaluación segura contiene la información necesitada para encriptar los datos, de acuerdo con más que un segundo método de encriptación.
15. Un sistema de evaluación segura como en la reivindicación 14, CARACTERIZADO porque dicha electrónica de control seguro selecciona el apropiado segundo método de encriptación, después de la evaluación de dichos datos no encriptados del titular de la tarjeta.

16. Un sistema de evaluación segura como en la reivindicación 14, CARACTERIZADO porque dicha memoria del sistema de evaluación segura contiene un archivo de configuración del sitio.
17. Un sistema de evaluación segura como en la reivindicación 12, CARACTERIZADO porque dicha electrónica de control seguro está contra la manipulación indebida.
18. Un sistema de evaluación segura como en la reivindicación 12, CARACTERIZADO porque dicha electrónica de control seguro comprende una memoria interna, almacenando la información necesitada para descryptar los datos encriptados, de acuerdo con dicho tercer método de encriptación.
19. Un sistema de evaluación segura como en la reivindicación 18, CARACTERIZADO porque dicha electrónica de control seguro está implementada como un chip USIP.
20. Un sistema de evaluación segura como en la reivindicación 18, CARACTERIZADO porque dicho tercer método de encriptación comprende el AES-128.
21. Un sistema de evaluación segura como en la reivindicación 12, CARACTERIZADO porque comprende, además, una interfaz USB.
22. Un sistema de evaluación segura como en la reivindicación 21, CARACTERIZADO porque dicho sistema de evaluación segura está ubicado en un dispositivo de manipulación de los datos del titular de la tarjeta.
23. Un sistema de evaluación segura como en la reivindicación 22, CARACTERIZADO porque dicho dispositivo de manipulación de los datos del titular de la tarjeta, es seleccionado entre el grupo que consta de un sistema de control del surtidor de combustible, un POS y un controlador de sitio.

24. Un sistema de evaluación segura como en la reivindicación 12, CARACTERIZADO porque dicha electrónica de control seguro transmite dichos datos no encriptados del titular de la tarjeta hacia un sistema de procesamiento local, en la forma no encriptada si dichos datos no encriptados del titular de la tarjeta son los datos no sensibles del titular de la tarjeta.
25. Un sistema de evaluación segura como en la reivindicación 12, CARACTERIZADO porque dicha electrónica de control seguro está adaptada ulteriormente, para evaluar dichos datos no encriptados del titular de la tarjeta, con el fin de realizar la validación de la transacción.
26. Un sistema de evaluación segura como en la reivindicación 25, CARACTERIZADO porque dicha memoria del sistema de evaluación segura contiene un archivo de registro de la transacción.
27. Un sistema de evaluación segura como en la reivindicación 12, CARACTERIZADO porque dicho sistema de evaluación segura está implementado como una CPU contra la manipulación indebida.
28. Un método para el procesamiento de una transacción, involucrando los datos del titular de la tarjeta en un sistema de pago minorista, CARACTERIZADO porque comprende los pasos de:

la recepción de los datos del titular de la tarjeta en un dispositivo de entrada;

la encriptación de dichos datos del titular de la tarjeta, de acuerdo con un primer método de encriptación, con el fin de producir los primeros datos encriptados del titular de la tarjeta;

la recepción de dichos primeros datos encriptados del titular de la tarjeta en un sistema de evaluación segura, acoplado a un dispositivo de manipulación de los datos del titular de la tarjeta;

la desencriptación de dichos primeros datos encriptados del titular de la tarjeta, con el fin de producir los datos no encriptados del titular de la tarjeta;

la evaluación de dichos datos no encriptados del titular de la tarjeta en una electrónica de control seguro, con el fin de determinar si dichos datos no

encriptados del titular de la tarjeta son los datos del titular de la tarjeta de pago, o los datos no sensibles del titular de la tarjeta; y

si dichos datos no encriptados del titular de la tarjeta son los datos del titular de la tarjeta de pago, encriptando dichos datos no encriptados del titular de la tarjeta, de acuerdo con un segundo método de encriptación, con el fin de producir los segundos datos encriptados del titular de la tarjeta.

29. El método según la reivindicación 28, CARACTERIZADO porque comprende, además, la transmisión de dichos datos no encriptados del titular de la tarjeta hacia un sistema de procesamiento local, en una forma no encriptada, si dichos datos no encriptados del titular de la tarjeta son los datos no sensibles del titular de la tarjeta.
30. El método según la reivindicación 28, CARACTERIZADO porque dicha electrónica de control seguro está contra la manipulación indebida.
31. El método según la reivindicación 28, CARACTERIZADO porque dichos primer y segundo métodos de encriptación son diferentes.
32. El método según la reivindicación 31, CARACTERIZADO porque comprende, además, la transmisión de dichos segundos datos encriptados del titular de la tarjeta hacia un sistema procesador anfitrión remoto.
33. El método según la reivindicación 28, CARACTERIZADO porque dicho dispositivo de manipulación de los datos del titular de la tarjeta, es seleccionado entre el grupo que consta de un sistema de control del surtidor de combustible, un POS y un controlador de sitio.
34. El método según la reivindicación 28, CARACTERIZADO porque comprende, además, la evaluación de dichos datos no encriptados del titular de la tarjeta en dicha electrónica de control seguro, con el fin de realizar la validación de la transacción.
35. El método según la reivindicación 28, CARACTERIZADO porque dicho sistema de evaluación segura está implementado como un candado electrónico teniendo una interfaz USB.

RESUMEN

Un sistema usado en un entorno minorista para la provisión de la encriptación de extremo a extremo de los datos del titular de la tarjeta de pago. Un dispositivo de entrada configurado para recibir los datos del titular de la tarjeta, está operativo para encriptar los datos del titular de la tarjeta, de acuerdo con un primer método de encriptación, con el fin de producir los primeros datos encriptados del titular de la tarjeta. Un dispositivo de manipulación de los datos del titular de la tarjeta está en comunicación electrónica con el dispositivo de entrada. Un sistema de evaluación segura (SEA) está operativamente conectado con el dispositivo de manipulación de los datos del titular de la tarjeta, y comprende la electrónica de control respecto a la manipulación indebida, adaptada para desencriptar los primeros datos encriptados del titular de la tarjeta, con el fin de producir los datos no encriptados del titular de la tarjeta. La electrónica de control respecto a la manipulación indebida evalúa los datos no encriptados del titular de la tarjeta, con el fin de determinar si los datos no encriptados del titular de la tarjeta son los datos del titular de la tarjeta de pago, o los datos no sensibles del titular de la tarjeta. Finalmente, si los datos no encriptados del titular de la tarjeta son los datos del titular de la tarjeta de pago, la electrónica de control respecto a la manipulación indebida del SEA está adaptada para encriptar los datos no encriptados del titular de la tarjeta, de acuerdo con un segundo método de encriptación, con el fin de producir los segundos datos encriptados del titular de la tarjeta.

2/6

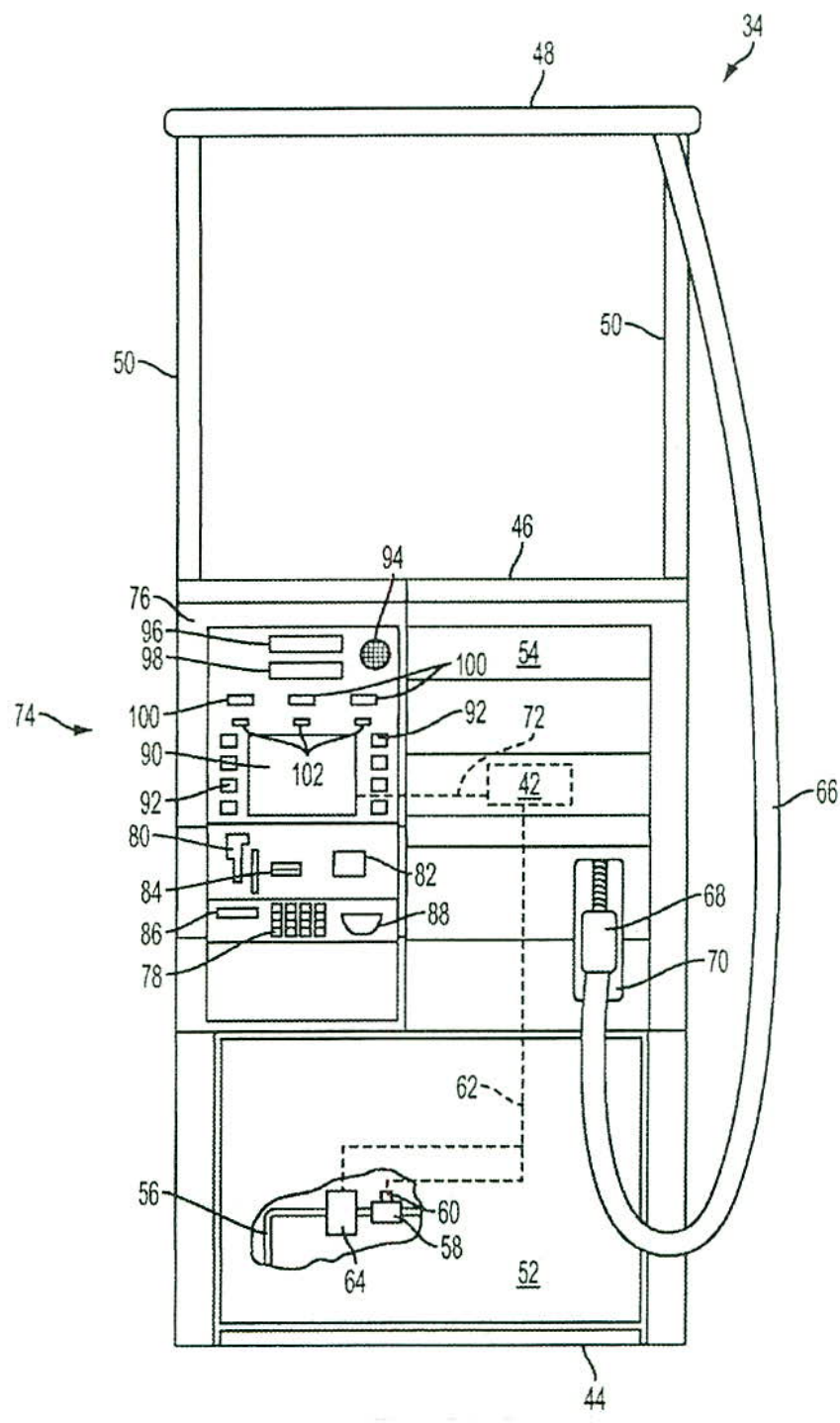


FIGURA 2

FIGURA 3

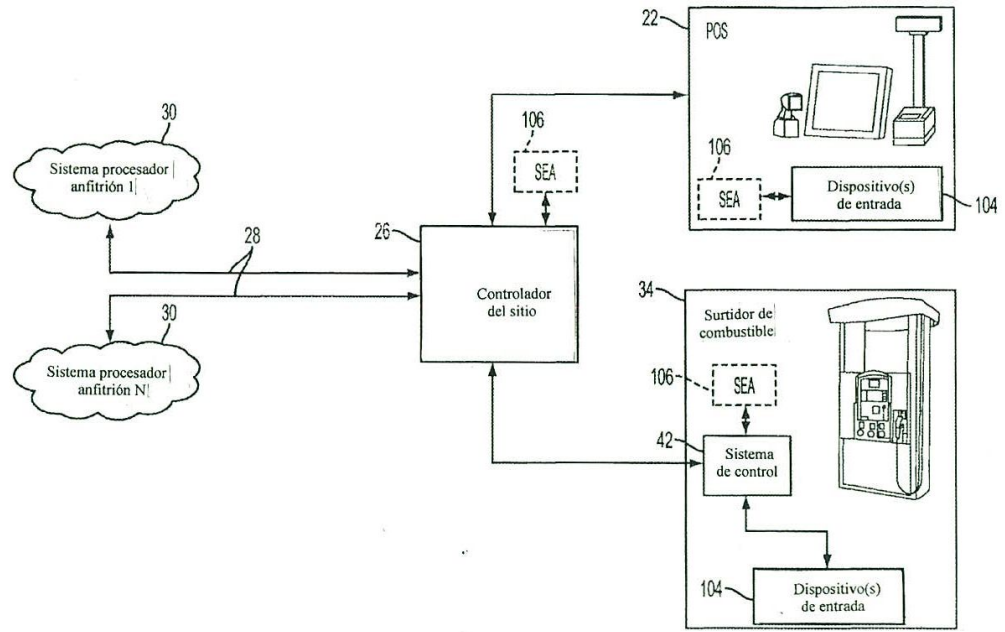
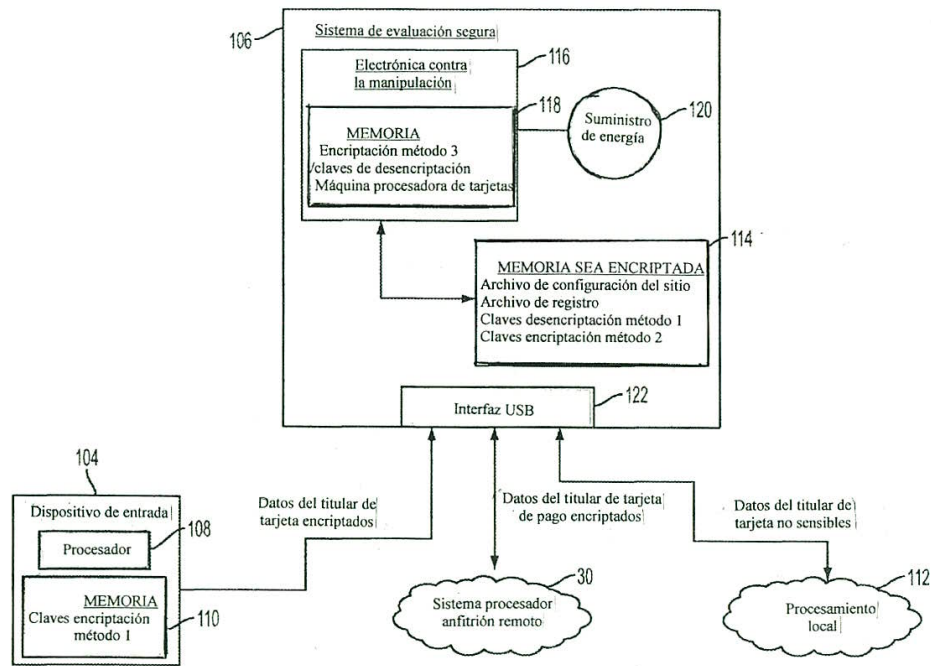


FIGURA 4



5/6

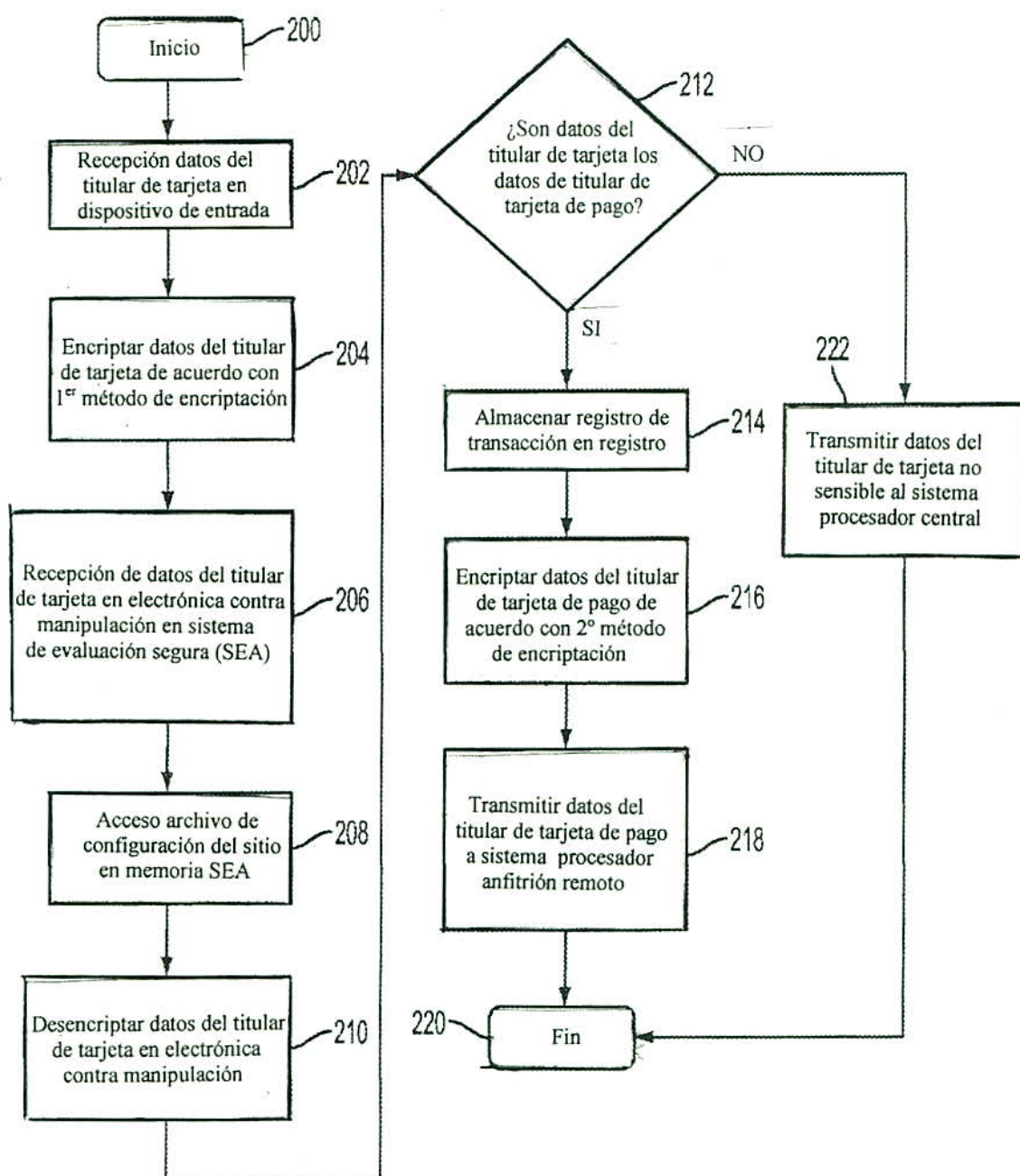


FIGURA 5

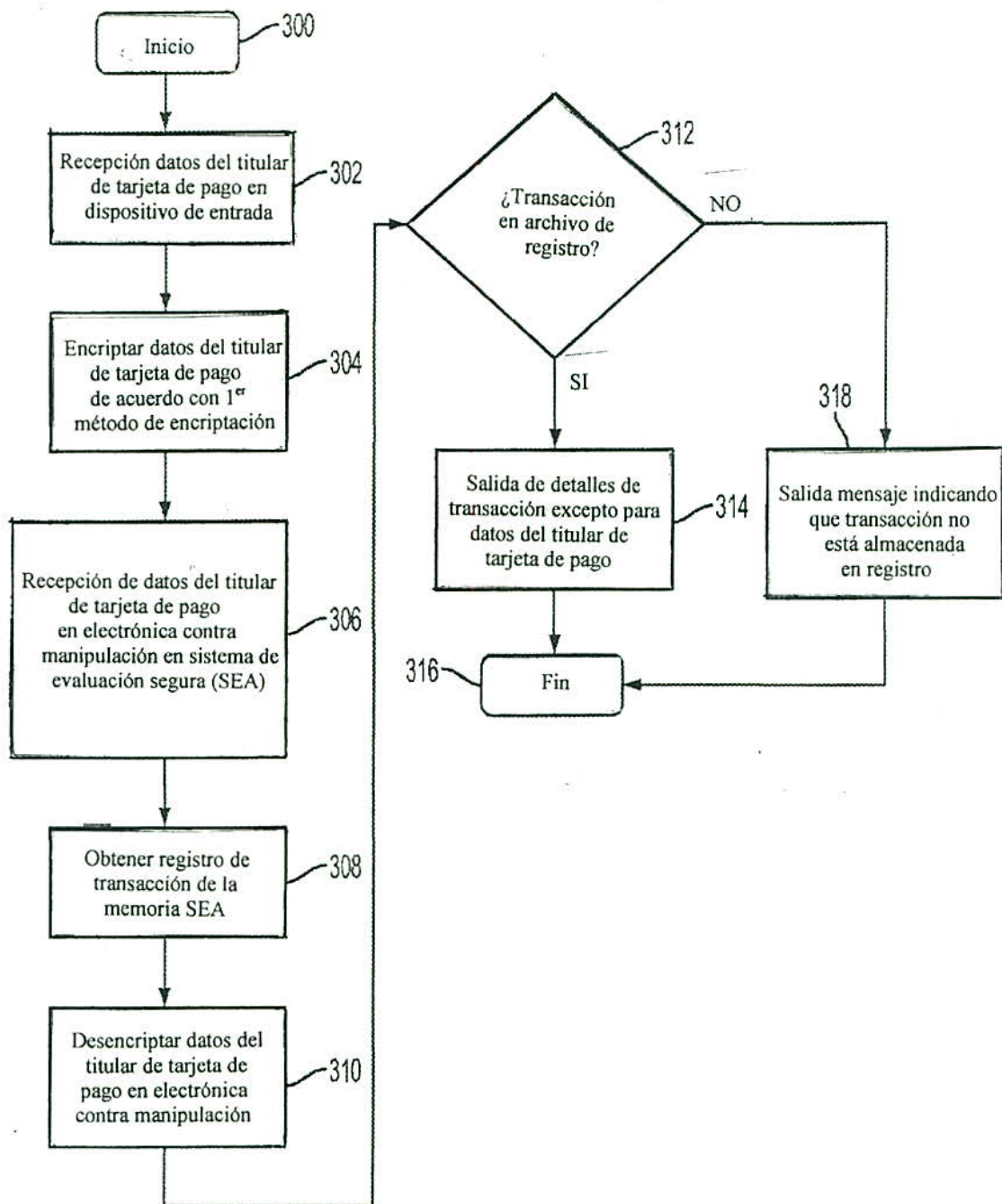


FIGURA 6

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

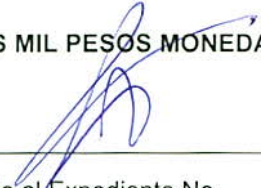
 Industria y Comercio SUPERINTENDENCIA	RECIBO DE CAJA	No. 13 - 0054513
		Bogotá D.C., Junio 06 de 2013 - 08:23:12

RECIBIDO DE : BRIGARD & CASTRO S.A. NI 860.047.372

*** Soporte del Pago ***					
TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	VR. PAGO
CONSIGNACION	BANCO DE BOGOTA	062754387	426513290	05/06/2013	21.138.000.00

*** Conceptos Pagados ***			
CANT.	RENTISTICO	CONCEPTO	
10 50005-01-01	SOLICITUDES	1607 REIVINDICACION PATENTE UNITARIA ADICIONAL A LAS 10 INIC	
			Vr.UNDITARIO Vr.CONCEPTO
			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. 13-169786- -00000-0000
Fecha: 2013-07-17 16:53:00 Dep. 2020 DIR.NUEVASCR
Tra. 11 PATENTEIYII Eve: 378 FASENACIONALI
Act. 411 PRESENTACION Folios: 49

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800.176.089-2

- / -



RECIBO DE CAJA

No. 13 - 0038199

Bogotá D.C., Abril 23 de 2013 - 16:26:25

RECIBIDO DE : BRIGARD & CASTRO S.A.

NI 860.047.372

*** Soporte del Pago ***

TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	VR. PAGO
CONSIGNACION	BANCO DE BOGOTA	062754387	426513264	23/04/2013	33.520.000.00

*** Conceptos Pagados ***

CANT.	RENTISTICO	CONCEPTO	Vr. UNDITARIO	Vr. CONCEPTO
15	50005-01-01 SOLICITUDES	1607 REIVINDICACION PATENTE UNITARIA ADICIONAL A LAS 10 INIC	30.000.00	450.000.00
				\$450.000.00

SON: **CUATROCIENTOS CINCUENTA MIL PESOS MONEDA CORRIENTE**

Responsable: 

Recibo de Caja Aplicado al Expediente No. _____

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 13-169786- -00000-0000

Fecha: 2013-07-17 16:53:00 Dep. 2020 DIR.NUEVASCR
Tra. 11 PATENTEIYII Eve: 378 FASENACIONALI
Act. 411 PRESENTACION Folios: 49

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

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

, Abril 23 de 2013 - 16:26:39

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

 Industria y Comercio SUPERINTENDENCIA	RECIBO DE CAJA	No. 13 - 0046829
		Bogotá D.C., Mayo 15 de 2013 - 16:51:49

RECIBIDO DE : BRIGARD & CASTRO S.A. NI 860.047.372

*** Soporte del Pago ***					
TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	VR PAGO
CONSIGNACION	BANCO DE BOGOTA	062754387	426513242	15/05/2013	57.807.000.00

*** Conceptos Pagados ***			
CANT.	RENTISTICO	CONCEPTO	
1	50005-01-01 SOLICITUDES	7 TTLOS-TRAMITES DE SOL. DE DISENOS INDUSTRIALES	
			Vr.UNDITARIO Vr.CONCEPTO
			500.000.00 500.000.00
			\$500.000.00
			=====

SON: **QUINIENTOS MIL PESOS MONEDA CORRIENTE**

Responsable: _____

Recibo de Caja Aplicado al Expediente No. _____

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

No. 13-169786- -00000-0000
Fecha: 2013-07-17 16:53:00 Dep. 2020 DIR.NUEVASCR
Tra. 11 PATENTEIYII Eve: 378 FASENACIONALI
Act. 411 PRESENTACION Folios: 49

PATENTE DE INVENCION ☐

MODELO DE UTILIDAD ☐

Art 33 Decisión 486/00

☐	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 ☐	

PI02-F08 (2009-11-18)

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 13-169786- -00000-0000

Fecha: 2013-07-17 16:53:00 Dep. 2020 DIR.NUEVASCR
Tra. 11 PATENTEIYII Eve: 378 FASENACIONALI
Act. 411 PRESENTACION Folios: 49