(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 445 151**

(51) Int. CI.:

G06Q 10/00 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **04.09.2003 E 03816988 (4)**

(97) Fecha y número de publicación de la concesión europea: **06.11.2013 EP 2143028**

(54) Título: **Gestión segura de un pin**

(30) Prioridad:

04.09.2002 US 408122 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.02.2014

(73) Titular/es:

ACCULLINK, INC. (50.0%)
3225 Cumberland Boulevard, Suite 550
Atlanta, GA 30339, US y
ZIEGLER, ROBERT (50.0%)

(72) Inventor/es:

ZIEGLER, ROBERT

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

DESCRIPCIÓN

Gestión segura de un pin.

Campo técnico de la invención

La presente invención se refiere a protocolos de seguridad, en particular para un proceso destinado a proteger una transacción financiera en línea, basada en números PIN.

Referencia cruzada a solicitudes relacionadas

Esta solicitud reivindica prioridad sobre la Solicitud Provisional US 60/408.122 titulada "SECURE PIN MANAGEMENT", presentada el 4 de septiembre de 2002. Esta solicitud hace referencia además a las Solicitudes de Patente US 09/874.274 titulada "SECURE KEY ENTRY USING A GRAPHICAL USER INTERFACE", presentada el 6 de junio de 2001, 09/874.261 titulada "CLIENT SYSTEM VALIDATION BY NETWORK ADDRESS AND ASSOCIATED GEOGRAPHIC LOCATION VERIFICATION", presentada el 6 de junio de 2001, y 10/264.762 titulada "SYSTEM AND METHOD FOR PROCESSING PIN-AUTHENTICATED TRANSACTIONS", presentada el 4 de octubre de 2002.

Antecedentes de la invención

El 92% de todas las transacciones en Internet se lleva a cabo con tarjetas de crédito. En el uso de las tarjetas de crédito surgen varios problemas, tanto desde la perspectiva del cliente como de los vendedores. Uno de los problemas más serios para muchos vendedores en línea proviene del hecho de que las transacciones con tarjetas de crédito se pueden recusar con una simple llamada telefónica. Uno de los motivos por los que las transacciones en Internet con tarjetas de crédito se pueden recusar de una manera tan sencilla y eficaz es que nunca se autentica al cliente. Particularmente cuando se trata de servicios, la incapacidad de verificar la identidad del cliente es un defecto importante en la naturaleza de las transacciones en línea con tarjetas de crédito.

Por otro lado, las transacciones con ATM o por tarjetas de débito, en las que la transacción se ha verificado con un PIN, no se pueden recusar. Al incluir la introducción del PIN en una transacción, se puede autenticar la identidad del cliente. No obstante, la red de EFT está gobernada por reglas diseñadas para salvaguardar a los diversos participantes de una transacción por ATM. En particular, la seguridad del PIN está sujeta a controles estrictos. Sin embargo, la mayoría de propuestas de introducir las ventajas de las transacciones por ATM en el entorno en línea no consigue una protección adecuada para que el PIN no se vea comprometido.

Algunas soluciones abordan el problema de la seguridad del PIN proponiendo la introducción de hardware seguro adicional y/o rutas de comunicación adicionales para cada ordenador de cliente. Estos tipos de soluciones introducen costes en el sistema que constituirán un obstáculo para la aceptación generalizada de la solución por parte del público en general.

Por lo tanto, se requieren un sistema y un método para proporcionar transacciones seguras basadas en PIN a través de Internet, sin la necesidad de hardware o líneas de comunicación adicionales para el cliente.

El documento US-A-5.363.449 da a conocer un método para cifrar un número de identificación personal seguro usando un terminal, un anfitrión y datos de terminal.

Sumario de la invención

Un sistema y un método de procesado seguro de PIN en una transacción en red incluyen un gestor de transacciones que envía datos de terminal a un terminal. El terminal genera datos corolarios a partir de la entrada del usuario y de los datos de terminal. Los datos corolarios se envían al gestor de transacciones. A continuación, el gestor de transacciones envía los datos corolarios y datos de HSM a un módulo de seguridad de hardware. El módulo de seguridad de hardware genera un PIN a partir de los datos corolarios y los datos de HSM, cifra el PIN y genera un bloque de PIN. El gestor de transacciones usa el bloque de PIN y datos de transacción para enviar una solicitud de transacción a la Red ATM.

Por consiguiente, en un aspecto de la presente invención se proporciona un método de procesado seguro de números de identificación personal (PIN) en una transacción en red entre un terminal y un servidor de comercio (en inglés, "merchant server"), en donde el servidor de comercio establece una conexión de red entre el terminal y un gestor de transacciones, de tal manera que el servidor de comercio no tiene conocimiento de datos intercambiados entre el terminal y el gestor de transacciones, comprendiendo el método las etapas de: generar datos de terminal que definen un secreto no compartido, por medio de un gestor de transacciones; generar datos de módulo de seguridad de hardware (HSM) que definen un secreto no compartido, por medio del gestor de transacciones; enviar datos de terminal desde el gestor de transacciones a un terminal; en donde el terminal genera una interfaz gráfica de introducción de PIN que comprende un teclado usando el secreto no compartido definido por los datos de terminal,

graba datos de posición del cursor que indican posiciones de cursor correspondientes a un cursor de ratón del terminal cuando el cursor del ratón se usa para seleccionar dígitos de un PIN por medio de la interfaz gráfica de introducción de PIN, genera datos corolarios en relación con el PIN usando el secreto no compartido definido por los datos de terminal y datos de posición del cursor, en donde el teclado se aleatoriza de tal manera que una posición dada del cursor del ratón indica un numeral diferente con cada dígito introducido; recibir en el gestor de transacciones datos corolarios desde dicho terminal; enviar datos corolarios y datos de módulo de seguridad de hardware (HSM) desde el gestor de transacciones a un módulo de seguridad de hardware; en donde el módulo de seguridad de hardware calcula el PIN basándose en los datos corolarios y los datos de HSM, y en donde el módulo de seguridad de hardware cifra el PIN y genera un bloque de PIN que incluye el PIN cifrado; recibir en el gestor de transacciones el bloque de PIN desde dicho módulo de seguridad de hardware, generar por medio del gestor de transacciones una solicitud de transacción que incluye dicho bloque de PIN y transmitir dicha solicitud de transacción desde el gestor de transacciones para la autenticación del PIN y la transacción; determinar en el gestor de transacciones si una entidad financiera ha autenticado la transacción; y notificar al servidor de comercio, por medio del gestor de transacciones, si se ha autenticado la transacción basándose en la etapa de determinación.

Preferentemente, en donde dichos datos de terminal incluyen algoritmos. Preferentemente, en donde dichos datos de terminal incluyen datos semilla. Preferentemente que comprende además la etapa de recibir datos de transacción desde el terminal y de incluir dichos datos de transacción en dicha solicitud de transacción.

En un segundo aspecto de la segunda invención se proporciona un sistema para el procesado seguro de números de identificación personal (PIN), que comprende: un gestor de transacciones para gestionar la transacción entre un terminal y un servidor de comercio, en donde el gestor de transacciones genera datos de terminal que definen un secreto no compartido, y en donde el gestor de transacciones genera datos de módulo de seguridad de hardware (HSM) que definen un secreto no compartido; un módulo de transacciones ejecutado por el terminal y conectado con capacidad de comunicación a dicho gestor de transacciones para recibir los datos de terminal desde el gestor de transacciones, generar una interfaz gráfica de introducción de PIN que comprende un teclado usando el secreto no compartido definido por los datos de terminal, grabar datos de posición de cursor que indican posiciones de cursor correspondientes a un cursor de ratón del terminal cuando el cursor del ratón se usa para seleccionar dígitos de un PIN por medio de la interfaz gráfica de introducción de PIN, generar datos corolarios en relación con el PIN usando el secreto no compartido definido por los datos de terminal y los datos de posición del cursor, y enviar los datos corolarios al gestor de transacciones, en donde el servidor de comercio no tiene conocimiento de datos intercambiados entre el terminal y el gestor de transacciones, en donde los datos de entrada del usuario se basan en entradas del usuario recibidas por el terminal y un módulo de seguridad de hardware conectado con capacidad de comunicación a dicho gestor de transacciones, para recibir los datos corolarios y los datos de HSM desde el gestor de transacciones, calcular el PIN basándose en los datos corolarios y los datos de HSM, cifrar el PIN y generar un bloque de PIN que incluye el PIN cifrado; en donde dicho gestor de transacciones recibe el bloque de PIN desde dicho módulo de seguridad de hardware, genera una solicitud de transacción que incluye dicho bloque de PIN, transmite dicha solicitud de transacción para la autenticación del PIN y la transacción, determina si una entidad financiera ha autenticado la transacción, y notifica al servidor de comercio si se ha autenticado la transacción.

Preferentemente, en donde dicho gestor de transacciones está conectado con capacidad de comunicación a dicho módulo de transacciones mediante una red abierta. Preferentemente, en donde dicho gestor de transacciones está conectado con capacidad de comunicación a dicho módulo de seguridad de hardware mediante una conexión directa. Preferentemente, en donde dichos datos de terminal incluyen un algoritmo.

Preferentemente, en donde dichos datos de HSM incluyen un algoritmo.

Breve descripción de los dibujos

Para entender de forma más completa la presente invención y sus ventajas, a continuación se hace referencia a la siguiente descripción considerada conjuntamente con los dibujos adjuntos, en los cuales:

la figura 1 ilustra un sistema de procesado seguro de PIN;
las figuras 2A y 2B ilustran un diagrama de flujo de comunicación de un sistema de procesado seguro de PIN; y
las figuras 3A-D ilustran un diagrama de flujo de un proceso de un sistema de procesado seguro de PIN.

Descripción detallada de la invención

Haciendo referencia a continuación a los dibujos, en los que los números de referencia iguales se usan para designar los mismos elementos en la totalidad de las diversas vistas, se describen adicionalmente varias formas de realización de la presente invención. Las figuras no se han dibujado necesariamente a escala, y, en algunos casos, los dibujos se han exagerado o simplificado únicamente con fines ilustrativos. Aquellos con conocimientos habituales en la materia apreciarán la multitud de posibles aplicaciones y variaciones de la presente invención basándose en los siguientes ejemplos de posibles formas de realización de la presente invención.

En referencia a la figura 1, se muestra un sistema de procesado seguro de PIN 100. De acuerdo con la forma de

realización preferida, el sistema de procesado seguro de PIN 100 actúa como parte de un proceso de transacción comercial en línea. Debería entenderse que el sistema de procesado seguro de PIN 100 se puede usar en otros entornos de transacciones en red, típicamente en procesos en los que un participante se debe autenticar sin la transferencia insegura de datos de autenticación. Un número de identificación personal (PIN) es una secuencia de numerales, donde el número de dígitos crea una probabilidad suficiente alta de que una persona poseedora del PIN se pueda identificar sin dudas como persona especificada. Lo más habitual es que los PIN se usen asociados a tarjetas bancarias de débito. Las tarjetas bancarias de débito se usan en cajeros automáticos (ATM) conectados a la Red de ATM. Cuando el cliente presenta la tarjeta al ATM, el ATM le pide al cliente que introduzca un PIN. El cliente introduce el PIN en el ATM. El ATM procesa el PIN y datos leídos de la tarjeta bancaria de débito para identificar al cliente que presenta la tarjeta como propietario legítimo de la misma. El proceso para transacciones basadas en PIN con tarjetas de débito en ATM está fuertemente regulado.

A efectos de la presente exposición, un PIN puede ser cualquier secuencia de números usados para realizar una identificación, particularmente cuando la identificación forme parte de una transacción. Puesto que la Red de ATM tiene requisitos específicos, la forma de realización preferida está adaptada a ese uso. Resultará evidente para aquellos expertos en la materia que se pueden usar los mismos protocolos en una amplia variedad de situaciones, particularmente situaciones en las que la identificación forma parte de una transacción en red. Las tarjetas de débito son solamente un ejemplo de *tokens* que pueden estar asociados a un PIN. Las tarjetas de crédito, las tarjetas de identificación, los llaveros, los teléfonos celulares, los asistentes personales digitales, los ordenadores, los ordenadores portátiles y los dispositivos informáticos, las tarjetas inteligentes y los transmisores pasivos o activos son ejemplos de tipos de *tokens* que se pueden identificar con un propietario por medio de un PIN. Los números de serie, las contraseñas, los parámetros biométricos, los números de identificación, los números de registro, los números de identificación de estudiante, las contraseñas de red, incluyendo numerales, caracteres o cualquier símbolo gráfico, son ejemplos de secuencias que pueden actuar como un PIN.

En el proceso de transacciones comerciales en línea, un cliente que está usando un terminal de cliente 104 se conecta a una red abierta 106 tal como Internet. El terminal de cliente 104 es preferentemente un ordenador personal que se usa en casa o en la oficina. Debería entenderse que el terminal de cliente 104 puede ser cualquier dispositivo digital que se pueda conectar con capacidad de comunicación a una red abierta 106 y que tenga capacidad de recibir datos introducidos por el cliente y de procesar los datos introducidos por el cliente antes de su transmisión a la red abierta 106.

Típicamente, el cliente que se encuentra en el terminal de cliente 104 se conecta a un servidor de comercio 108 por medio de Internet 106. El servidor de comercio 108 puede ofrecer al cliente artículos o servicios a la venta, con una o más páginas web que actúan como interfaces de consumidor. Cuando el cliente ha realizado las selecciones apropiadas en el sitio web de comercio, al mismo se le ofrecen típicamente opciones de pago. La comunicación entre el terminal de cliente 104 y el servidor de comercio 108 se llevará a cabo típicamente usando un enlace de capa de conexión segura (SSL), aunque la seguridad de la comunicación de la transacción se puede materializar de acuerdo con otro protocolo o incluso se puede hacer abierta, en función de las necesidades de seguridad dictaminadas por las transacciones y los protocolos específicos. De acuerdo con la presente forma de realización, cuando se selecciona una transacción de tipo débito en la que se transfiere dinero desde una cuenta bancaria de cliente en una entidad financiera 120 por medio de la red de ATM 118, se inicia la transacción, típicamente por medio de un mensaje de inicio de transacción enviado desde el terminal de cliente 104, a través de la red abierta 106, al servidor de comercio 108.

Cuando se recibe un mensaje de inicio de transacción en el servidor de comercio 108, el servidor de comercio 108 comunica el inicio de transacción, que incluye detalles de la transacción, detalles del vendedor y detalles del cliente, al gestor de transacciones 102. Las comunicaciones entre el servidor de comercio 108 y el gestor de transacciones 102 se efectúan típicamente usando una red de comunicaciones dedicada o una red privada virtual (VPN). Algunas comunicaciones entre el servidor de comercio 108 y el gestor de transacciones 102 se pueden llevar a cabo por medio de la red abierta 106, aunque, debido al carácter confidencial de la transacción financiera, la comunicación entre el servidor de comercio 108 y el gestor de transacciones 102 usará típicamente una conexión segura.

El servidor de comercio 108 establecerá una conexión entre el terminal de cliente 104 y el gestor de transacciones 102. Esta conexión se establecerá típicamente de tal manera que el cliente en el terminal de cliente 104 en general desconozca que el cliente se está comunicando con el gestor de transacciones 102 en lugar del servidor de comercio. No obstante, una vez que se ha establecido la conexión entre el terminal de cliente 104 y el gestor de transacciones 102, el servidor de comercio 108 no tiene conocimiento de ninguno de los datos intercambiados entre el terminal de cliente 104 y el gestor de transacciones 102. Este protocolo evita que el servidor de comercio 108 intercepte las comunicaciones entre el terminal de cliente 104 y el gestor de transacciones 102 y que obtenga acceso a datos financieros o personales confidenciales, al mismo tiempo que evita ataques del tipo hombre en el medio en el sistema.

El gestor de transacciones 102 está conectado con capacidad de comunicación a una base de datos de gestor de transacciones 112. La base de datos de gestor de transacciones 112 almacena algoritmos y otros datos usados en las transacciones. Cuando el terminal de cliente 104 inicia una primera transacción, el gestor de transacciones 102

recupera una copia de un módulo de transacción a partir de la base de datos del gestor de transacciones 112 y envía un módulo de transacción al terminal de cliente 104. El módulo de transacción protege el terminal de cliente 104 y regula el proceso de transacción en el terminal de cliente 104. La base de datos de gestor de transacciones 112 puede almacenar algoritmos usados para generar una interfaz dinámica de introducción de PIN, algoritmos de cifrado, componentes de algoritmos de cifrado y otros datos usados como secretos no compartidos. Los algoritmos y datos almacenados en la base de datos de gestor de transacciones se pueden organizar en familias de datos, de tal manera que cuando haya disponible una familia de DDA para un módulo de transacciones, las etapas de procesado se pueden seleccionar identificando partes de la familia de DDA y con datos para determinar las variables usadas en la creación de datos corolarios.

El gestor de transacciones 102 está conectado, con capacidad de comunicación, a una interfaz de Módulo de Seguridad de Hardware (HSM) 110. La interfaz de HSM 110 puede ser un terminal de configuración segura (SCT). La conexión entre el gestor de transacciones 102 y la interfaz de HSM 110 es típicamente una conexión de línea protegida. La interfaz de HSM 110 está conectada directamente a un HSM 114. El HSM 114 o la interfaz de HSM 110 puede incluir un lector de tarjetas 115 para leer datos de una tarjeta llave 116.

De acuerdo con la forma de realización preferida, el Módulo de Seguridad de Hardware 114 es un HSM programable o inteligente. Un HSM programable es, en general, un HSM que tiene la capacidad de interpretar datos inyectados, como instrucciones programáticas. Instrucciones programáticas puede referirse a imágenes ejecutables tales como una aplicación escrita en un lenguaje de programación tal como código ensamblador, C o C++. Como instrucciones programáticas pueden usarse imágenes de tiempo de ejecución tales como una aplicación JAVA.

Mediante la programación del HSM inteligente, el HSM puede implementar un comportamiento programado de forma o bien estática o bien dinámica. De esta manera, el HSM se puede programar para interaccionar de forma segura con las funciones criptográficas del HSM. Se pueden descargar aplicaciones en el HSM usando cualquier metodología segura. Por ejemplo, las aplicaciones se pueden introducir en el HSM usando un puerto serie, un adaptador de red, tarjetas inteligentes, discos flexibles, cd-roms, un puerto de infrarrojos o cualquier otro mecanismo de introducción conocido. De acuerdo con la forma de realización preferida, se puede usar una tarjeta inteligente 116 para inyectar algoritmos, claves u otros datos seguros en el HSM 114.

El código ejecutable inyectado en el HSM 114 se autentica típicamente usando una firma digital del código ejecutable generado por un editor autorizado. Pueden usarse otros métodos de autenticación. La imagen ejecutable, cuando se ejecuta, está programada de manera que se intercambian datos entre el HSM 114, la interfaz de HSM 110 y otros sistemas conectados, de una manera segura. En particular, la programación evita que se ponga en peligro el HSM 114 incluyendo los algoritmos y claves almacenados en el mismo. El HSM 114, de acuerdo con la forma de realización preferida, tiene la capacidad tanto de leer como de escribir en la tarjeta inteligente 116.

El HSM 114 es, de acuerdo con la forma de realización preferida, un Módulo de Seguridad Resistente a Manipulaciones (TRSM), que evita una intrusión tanto física como lógica. Usando componentes de software homologados, un terminal de configuración segura (SCT) personalizado, definiciones de ACL, políticas y procedimientos, se puede conseguir que el HSM programable 114 satisfaga los requisitos de gestión de claves X9. En particular, el HSM 114 puede materializar claves para intercambio de claves, gestión de claves con conocimiento parcial, control dual, fragmentos de claves, generación de pares de claves, inyección de claves, combinación de claves, intercambio de claves, carga de claves, recuperación de claves, destrucción de material de claves, gestión de claves con claves cifradas, creación de bloques de PIN, traducción de bloques de PIN, y gestión de PIN con números PIN cifrados, que sean compatibles con el X9. El HSM 114 puede ser un cerramiento a prueba de manipulaciones indebidas, que sea compatible con el X9, con destrucción de claves cuando la integridad del cerramiento del HSM se vea comprometida. Se hace que las políticas y procedimientos para estos procesos sean auditables y verificables.

El HSM 114 puede estar contenido en una caja duradera, resistente a manipulaciones, para proteger el sistema contra intrusiones, con características de detección incorporadas capaces de detectar intentos sofisticados de manipulaciones físicas o electrónicas. Un intento no autorizado de acceder al HSM da como resultado el borrado inmediato y automático de los algoritmos y datos protegidos almacenados en el HSM 114. El HSM 114 es un TRSM con capacidad de hacer cumplir la confidencialidad y separación de claves. El HSM 114 permite un control dual, una detección de manipulaciones y contramedidas activas, tales como el borrado automático de claves cuando su integridad se ve comprometida. Estos tipos de dispositivos y medidas de seguridad del entorno existen actualmente en muchos sistemas de entidades financieras, centros de procesado de redes e instalaciones militares.

El HSM 114 también puede usar listas de control de acceso para permitir un control minucioso sobre la separación de claves, la inyección de claves y la gestión de claves. El HSM 114 se programará preferentemente de manera que únicamente aceptará código de confianza autenticado proporcionado por un editor de confianza autenticado. La autenticación del código de confianza y el auditor de confianza se logra típicamente usando un protocolo apropiado de autenticación de firmas digitales.

El HSM 114 se puede programar para negarse a cargar código de confianza durante procesos de carga de claves.

El HSM 114 se puede programar para restringir la carga de código de acuerdo con procedimientos de auditoría X9. El HSM 114 debería superar los requisitos de validación FIPS-140. El HSM 114, conjuntamente con un SCT y prácticas homologadas de gestión de claves permiten la gestión de claves para su inyección en dispositivos que están separados física o geográficamente, según se pueda requerir para lograr las mejores prácticas en cuanto a continuidad del negocio. El HSM 114, conjuntamente con un SCT, puede cumplir o superar todas las prácticas de gestión de claves, requeridas por las directrices de auditoría TG-3 X9 o normativas asociadas.

Para conseguir que el HSM 114 sea compatible con requisitos X9, el HSM programado 114 requiere que las claves privadas y las claves simétricas se encuentren en un formato seguro aceptable. Las claves se pueden representar como texto en claro dentro de la memoria protegida de un módulo de seguridad resistente a manipulaciones, o cifradas cuando se representen fuera de la memoria protegida de un módulo de seguridad resistente a manipulaciones. Las claves se pueden representar en forma de dos o más fragmentos de clave o componentes de clave ya sea en texto en claro o en texto cifrado y se pueden gestionar usando un control dual con fragmentación de las claves con conocimiento parcial. Los secretos compartidos permiten que los fragmentos de clave se almacenen independientemente en *tokens* de manera que se requiere una cantidad menor que la totalidad de los fragmentos de clave (k-de-n fragmentos de clave) para cargar o recomponer la clave que se está protegiendo. Una buena práctica de seguridad requiere separación de claves, por la cual cada clave o par de claves se genera para una finalidad particular y se usa meramente para el fin para el cual estaba destinado.

La interfaz de HSM 110 se puede comunicar por interfaz directa o indirectamente con el HSM 114 para cargar la clave de cifrado de claves (KEK), pares de claves así como cualquier otra actividad necesaria para cumplir las normas X9 para gestión de claves. Por consiguiente, la interfaz de HSM 110 se puede conectar directamente al HSM 114, por ejemplo usando una SCSI, un IDE, un puerto serie, un puerto paralelo, un puerto USB, un teclado, un ratón, o un puerto *firewire*. La interfaz de HSM 110 se puede conectar indirectamente al HSM 114, por ejemplo usando un puerto de infrarrojos. La interfaz de HSM 110 puede tener capacidad de interfuncionamiento con el HSM 114 por medio del uso de tarjetas inteligentes con procesos y procedimientos de soporte para garantizar que se pueden implementar políticas y procedimientos de gestión de claves. También se pueden usar futuras metodologías de conexión, que se correspondan con las normas requeridas.

La interfaz de HSM 110 puede estar contenida en una caja duradera, resistente a manipulaciones, para salvaguardar el sistema contra incursiones. La interfaz de HSM 110 también debería incluir técnicas de detección incorporadas, con capacidad de detectar intentos sofisticados de manipulaciones físicas o electrónicas. Estas técnicas pueden proporcionar un borrado inmediato y automático de algoritmos y datos protegidos almacenados en el dispositivo.

De acuerdo con una forma de realización, la interfaz de HSM 110 puede proporcionar una pantalla gráfica, que le permita soportar una variedad de conjuntos de caracteres gráficos, incluyendo idiomas basados en japonés, chino, árabe y cirílico. La pantalla se puede configurar para mostrar dos líneas de indicadores de entrada (*prompts*) en chino, dos líneas de caracteres grandes o hasta cuatro líneas de texto en caracteres latinos. La interfaz de HSM 110 puede tener la capacidad de visualizar dos idiomas simultáneamente, tales como francés e inglés, para su uso en entornos multilingües.

La interfaz de HSM 110 se puede configurar para soportar un desarrollo de aplicaciones personalizado y una descarga remota de una imagen ejecutable. Típicamente, el proceso de descarga requerirá una fuente de código de confianza y el uso de código ejecutable que esté autenticado, a través de un certificado digital, *hash*, MAC u otra metodología suficiente para demostrar la autenticidad e integridad del código ejecutable.

La interfaz de HSM 110 puede proporcionar control de acceso usando tarjetas inteligentes, dispositivos *token*, contraseñas u otra metodología. El control de acceso se usa para garantizar que las descargas de código únicamente se pueden lograr por medio de entidades de confianza autorizadas. El uso de la interfaz de HSM 110 se puede restringir usando un control de acceso. La carga de claves se limita a participantes autorizados que usen un control de acceso. La inyección de claves se limita a participantes autorizados que usen un control de acceso. La descarga de software se limita a protocolos privativos y se limita alternativamente usando un control de acceso.

La interfaz de HSM 110 garantiza que el acceso a cualquier información de claves introducida no se puede controlar o denegar para uno o la totalidad de usuarios del HSM 114. La interfaz de HSM 110 garantiza que el acceso a cualquier información de claves introducida no se puede controlar o denegar para uno o la totalidad de usuarios del HSM 114. La interfaz de HSM 110 puede proporcionar una interfaz para el HSM 114. La interfaz de HSM 110 puede proporcionar soporte simultáneo para múltiples funciones de gestión de claves. La interfaz de HSM 110 puede proporcionar una seguridad exhaustiva por software y una caja a prueba de manipulaciones. La interfaz de HSM 110 puede almacenar claves de forma segura en un chip de seguridad. La interfaz de HSM 110 puede incluir la capacidad de borrar claves del chip de seguridad al completarse la actividad de las claves, si ello fuera necesario. La interfaz de HSM 110 puede proporcionar comunicaciones seguras entre un teclado, una pantalla y un módulo de seguridad. La interfaz de HSM 110 puede proporcionar un teclado para PIN, que soporte la introducción de caracteres alfanuméricos. La interfaz de HSM 110 puede proporcionar un lector y un dispositivo de escritura de tarjetas inteligentes que soporten una pluralidad de tarjetas con memorias protegidas y memorias asíncronas y

síncronas. La interfaz de HSM 110 puede incluir un lector de bandas magnéticas que pueda leer y escribir la Pista 1 y 2 o la Pista 2 y 3. La interfaz de HSM 110 puede proporcionar una interfaz serie.

El lector de tarjetas inteligentes y magnéticas 115 de la interfaz de HSM 110 puede proporcionar una característica de borrado segura y verificable para garantizar que no queda ningún material residual de claves después de que se haya producido una inyección de claves o se haya descartado material de las mismas. Esto se puede implementar como un procedimiento que requiera una ejecución y verificación, a un nivel sustancial, del borrado del material. El lector y dispositivo de escritura de tarjetas 115 puede soportar el EMV tanto para soporte de tarjetas inteligentes, tarjetas de débito, tarjetas de crédito, como tarjetas ATM.

La interfaz de HSM 110 puede ser segura desde el punto de vista tanto físico como electrónico, y puede contener un módulo de seguridad integral, con un chip de cifrado, que ofrezca soporte simultáneo para funciones de cifrado y de gestión de claves. Se puede prever que el módulo de seguridad trabaje con DES, Triple DES, cifrado RSA, y que soporte Clave Maestra/de Sesión, DUKPT (clave obtenida única por transacción) y métodos de gestión regional de claves.

La interfaz de HSM 110 puede proporcionar características adicionales que no sean necesarias para proteger el HSM 114, en la medida en la que el dispositivo puede incluir capacidades de utilidad de nivel superior para actuar como teclado para números PIN en transacciones de débito en línea y fuera de línea.

La interfaz de HSM 110 está conectada, con capacidad de comunicación, típicamente mediante una conexión de línea segura, a una red cerrada 118, tal como la Red ATM. Esta red cerrada 118 proporciona comunicación a una o más entidades financieras 120. La transacción correspondiente a la transferencia de cantidades de dinero desde una cuenta a otra se lleva a cabo mediante comunicaciones transmitidas a través de la Red ATM 118.

En sistemas típicos de la técnica anterior, al usar criptografía basada en software, todos los componentes criptográficos (es decir, el algoritmo, la clave, el texto en claro, el texto cifrado) residen en una memoria no protegida, en donde son susceptibles de sufrir duplicación, modificación, o sustitución. El elemento con mayor susceptibilidad es la clave criptográfica. Una clave duplicada permite que un atacante recupere todos los datos cifrados. Adicionalmente, una clave privada asimétrica duplicada permite que un enemigo genere falsamente firmas digitales que serían atribuidas al propietario del ordenador. Una clave pública sustituida o modificada permitiría un ataque del tipo “hombre en el medio” de tal manera que el enemigo podría interceptar y cambiar correos electrónicos o datos de transacciones, no detectables por el emisor o receptor.

En la criptografía basada en hardware, las barreras físicas y lógicas limitan el acceso a datos, mientras que el algoritmo y la clave se mantienen seguros en la memoria protegida del HSM 114. De este modo, la criptografía basada en hardware garantiza la confidencialidad, la integridad, y la autenticidad de claves criptográficas y, además, proporciona confianza en relación con la integridad y la autenticidad del algoritmo criptográfico, lo cual refuerza el nivel global de seguridad.

El sistema de procesado seguro de PIN 100 garantiza las políticas, prácticas y controles de ciclos de vida en la gestión de claves, que hacen frente a las políticas y prácticas de una organización en relación con la gestión de claves asimétricas privadas, claves simétricas, y otros tipos de material de claves (por ejemplo, valores semilla de un generador de números seudoaleatorios), incluyendo la gestión de hardware criptográfico. La información de control de los ciclos de vida en la gestión de claves se debería dar a conocer para permitir que los participantes que tienen confianza valoren si la organización mantiene controles suficientes para satisfacer sus requisitos de negocios y garantizar prácticas de generación de claves, de manera tal que se generen claves criptográficas de acuerdo con los estándares industriales.

El sistema de procesado seguro de PIN 100 gestiona el proceso de generación de números aleatorios o seudoaleatorios, la generación de números primos, los algoritmos de generación de claves, y los componentes de hardware y software. El sistema de procesado seguro de PIN mantiene fidelidad con todos los estándares relevantes así como referencias a la documentación procedimental de generación de claves incluyendo el almacenamiento y la copia de seguridad de claves. Las claves privadas asimétricas y las claves simétricas permanecen secretas, y se pueden conservar sus prácticas de integridad, autenticidad y recuperación. El sistema de procesado seguro de PIN 100 permite el uso de mecanismos de separación de claves usando componentes de hardware y software. Esto permite una fidelidad demostrable a todos los estándares relevantes y proporciona referencias a procedimientos de almacenamiento, de copias de seguridad, y de recuperación de claves. El sistema de procesado seguro de PIN 100 controla los procesos de distribución inicial de claves, los procesos subsiguientes de sustitución de claves, y los mecanismos de sincronización de claves.

El sistema de procesado seguro de PIN 100 se basa en el HSM 114 no solamente por motivos de seguridad, sino también para garantizar que la criptografía, la cual es intensiva en cuanto a la CPU, se optimiza en relación con una alta escalabilidad y tiene la capacidad de soportar diversas aplicaciones. El sistema y el proceso de procesado seguro de PIN 100 pueden hacer que se incremente drásticamente el número de claves criptográficas generadas, distribuidas, instaladas, usadas, y finalmente terminadas. Esta proliferación estresará la escalabilidad de software de

gestión de claves y los mecanismos de almacenamiento de claves que se verán obligados a gestionar cada vez más claves criptográficas.

En referencia a las Figuras 2A y 2B, se muestra un diagrama de flujo de comunicación para el proceso seguro de PIN 200. Cuando se ejecuta el módulo de transacciones, el mismo lleva a cabo un procedimiento para proteger el terminal de cliente 104 en la etapa 202. El proceso para proteger el terminal de cliente 104 puede incluir comprobar la ubicación, el registro y la memoria del terminal de cliente 104. El módulo de transacciones realiza una comprobación para observar si existe alguna indicación de que el proceso de transacción se puede volver inseguro por el cliente, el software de cliente o el hardware de cliente. Se lleva a cabo una exploración de puertos. Se comprueban interrupciones y vectores del terminal de cliente 104. El módulo de transacciones realiza una búsqueda de *crackers* de hardware. El objetivo es garantizar que el terminal de cliente 104 es un ordenador genérico que ejecuta software genérico. Si el módulo de transacciones determina que el terminal de cliente 104 es por algún motivo inseguro, se hace finalizar el proceso de la transacción.

Cuando se determina que el terminal de cliente es seguro, el módulo de transacciones envía datos de transacción al gestor de transacciones 102 en la etapa 204. Parte o la totalidad de los datos de transacción puede ser enviada por el gestor de transacciones 102 a la interfaz de HSM 110 en la etapa 212. Parte o la totalidad de los datos de transacción también puede ser enviada por la interfaz de HSM 110 al HSM 114. Los datos de transacción específicos compartidos por el módulo de transacciones, el gestor de transacciones 102, la interfaz de HSM 110 y el HSM 114 dependen de los detalles de los protocolos que se estén aplicando.

El módulo de transacciones solicita del terminal del gestor de transacciones 102 secretos no compartidos en la etapa 206. Típicamente, el gestor de transacciones 102 envía un desafío de autenticación al módulo de transacciones en la etapa 210. En la etapa 214 el módulo de transacciones envía una respuesta de autenticación al gestor de transacciones 102. El intercambio de datos de autenticación se puede llevar a cabo de varias maneras. La autenticación puede ser bidireccional, de tal manera que el módulo de transacciones se autentique para el gestor de transacciones 102 y el gestor de transacciones 102 se autentique para el módulo de transacciones. La autenticación puede tener lugar en otros momentos durante el proceso, y se puede repetir en algunos protocolos. Puesto que la identidad de los participantes es especialmente importante en una transacción financiera, para lograr ese objetivo se puede implementar una amplia variedad de protocolos y procedimientos de autenticación.

El gestor de transacciones 102 genera secretos no compartidos del terminal en la etapa 218 y secretos no compartidos del HSM en la etapa 220. Los secretos no compartidos del terminal se usan para permitir que el módulo de transacciones forme y codifique apropiadamente datos corolarios usados para identificar el PIN del cliente. Los secretos no compartidos del HSM son usados por el HSM 114 para convertir los datos corolarios en el PIN del cliente. Los secretos no compartidos pueden incluir algoritmos, partes de algoritmos, familias de algoritmos, identificadores para seleccionar algoritmos, partes de algoritmos o familias de algoritmos. Los secretos no compartidos pueden incluir datos para modificar los algoritmos. Los secretos no compartidos pueden establecer variables.

El gestor de transacciones 102 envía los secretos no compartidos del terminal al módulo de transacciones y envía los secretos no compartidos del HSM al HSM 114. El módulo de transacciones genera una interfaz gráfica de introducción de PIN para su visualización en el terminal de cliente 104 usando los secretos del terminal no compartidos en la etapa 222. El cliente selecciona partes visualizadas de la interfaz gráfica de introducción de PIN usando un ratón para generar datos de posición del cursor en la etapa 224. De acuerdo con la forma de realización preferida, la interfaz gráfica de introducción de PIN incluye una pantalla gráfica de un teclado numérico, de tal manera que el cliente selecciona un dígito del PIN haciendo clic en un botón del ratón cuando el cursor del ratón está sobre el número apropiado. Con cada dígito introducido, el teclado visualizado se puede aleatorizar, de tal manera que una posición dada del cursor del ratón puede indicar un numeral diferente con cada dígito introducido. Los datos de posición del cursor para cada dígito del PIN se graban por medio del módulo de transacciones. A continuación, el módulo de transacciones genera datos corolarios usando los datos de posición del cursor y los secretos del terminal no compartidos en la etapa 226. Los datos corolarios se envían al gestor de transacciones 102 el cual además envía los datos corolarios a la interfaz de HSM 110.

La interfaz de HSM 110 inyecta datos dinámicos en el HSM 114 usando los secretos no compartidos del HSM en la etapa 228. La interfaz de HSM 110 inyecta los datos corolarios en el HSM 114 en la etapa 230. El HSM 114, usando los datos de transacción 216, los datos dinámicos 232 y los datos corolarios 234, calcula el PIN de cliente en la etapa 236.

El HSM 114 cifra el PIN en la etapa 238. El HSM 114 genera un bloque de PIN usando el PIN cifrado y datos de transacción en la etapa 240. El HSM 114 envía el bloque de PIN a la interfaz de HSM 110 en la etapa 242. La interfaz de HSM 110 genera una solicitud de transacción que incluye el bloque de PIN en la etapa 244, y envía la solicitud de transacción a la Red ATM 118. La Red ATM 246 o la entidad financiera 120 autentica el PIN en la etapa 246. La entidad financiera 120 autentica la transacción en la etapa 248. A continuación, la entidad financiera 120 genera un mensaje de aprobación de transacción en la etapa 250, y envía el mensaje de aprobación de transacción al gestor de transacciones 102 en la etapa 252. El gestor de transacciones 102 notifica al servidor de comercio de

que se ha procesado la transacción.

En referencia a las Figuras 3A, 3B, 3C y 3D, se muestra un diagrama de flujo del proceso de procesado seguro de PIN 300. El proceso comienza cuando se inicia la transacción en el bloque de función 302. Se lleva a cabo una comprobación para determinar si el módulo de transacciones se ha instalado en el terminal de cliente 104, en el bloque de decisión 304. Si no se ha instalado ningún módulo de transacciones, el proceso sigue la ruta NO hacia el bloque de función 306, enviando una solicitud de módulo de transacciones al gestor de transacciones 102. El gestor de transacciones 102 recupera el archivo del módulo de transacciones a partir de la base de datos de gestor de transacciones 112 y carga el módulo de transacciones en el terminal de cliente 104, en el bloque de función 308, y prosigue hacia el bloque de función 310.

Si el módulo de transacciones estaba instalado previamente, el proceso sigue la ruta SÍ hacia el bloque de función 310. En el bloque de función 310, el terminal de cliente 104 ejecuta el módulo de transacciones. A continuación, el módulo de transacciones protege el terminal de cliente 104 en el bloque de función 312. Se lleva a cabo una comprobación para determinar si el terminal de cliente 104 es seguro, en el bloque de decisión 314. Si el terminal de cliente no es seguro, el proceso sigue la ruta NO hacia el bloque de función 316 en donde se le niega la transacción. A continuación, el proceso finaliza en el bloque 500.

Si se determina que el terminal de cliente es seguro, el proceso sigue la ruta SÍ hacia el bloque de función 316. El módulo de transacciones envía una solicitud de transacción al gestor de transacciones 102 en el bloque de función 316. El gestor de transacciones 102 envía un desafío de autenticación al módulo de transacciones en el bloque de función 318. El módulo de transacciones envía una respuesta de autenticación al gestor de transacciones 102 en el bloque de función 320. Si no se verifica la autenticación, la transacción se deniega. El módulo de transacciones solicita algoritmos y datos dinámicos en el bloque de función 322. El gestor de transacciones genera algoritmos y datos dinámicos de terminal que incluyen secretos no compartidos del terminal en el bloque de función 324.

El gestor de transacciones 102 genera algoritmos y datos dinámicos (DDA) de HSM que incluyen secretos no compartidos de HSM en el bloque de función 326. El módulo de transacciones genera una interfaz gráfica de introducción de PIN usando algoritmos y datos dinámicos de terminal que incluyen secretos no compartidos del terminal en el bloque de función 328. En el bloque de función 330 el terminal de cliente 104 visualiza la interfaz dinámica de introducción de PIN. El usuario hace clic en el botón del ratón en correspondencia con la posición de un cursor sobre dígitos visualizados en la interfaz dinámica de introducción de PIN en el bloque de función 332. En el bloque de función 334, el módulo de transacciones graba los datos de posición del cursor. En el bloque de función 336, el módulo de transacciones genera datos corolarios usando los algoritmos y datos dinámicos y los datos de posición del cursor.

El módulo de transacciones genera un mensaje de transacción que incluye datos de la transacción y datos corolarios en el bloque de función 338. Prosiguiendo hacia el bloque de función 340, el módulo de transacciones envía el mensaje de transacción al gestor de transacciones 102. El gestor de transacciones envía los algoritmos y datos dinámicos y los datos corolarios a la interfaz de HSM 110 en el bloque de función 342. En el bloque de función 344, la interfaz de HSM 110 inyecta los algoritmos y datos dinámicos del HSM, los datos semilla y los datos corolarios en el HSM 114. Prosiguiendo hacia el bloque de función 346, el HSM 114 calcula el PIN de cliente, basándose en los algoritmos, los datos semilla y los datos corolarios. El HSM 114 cifra el PIN usando una clave de cifrado de claves inyectadas en el bloque de función 348. El HSM 114 puede cifrar el PIN usando cualquiera de entre una variedad de técnicas de cifrado. De acuerdo con la forma de realización preferida, el cifrado se lleva a cabo usando una clave con conocimiento parcial, y control dual, que ha sido inyectada en el HSM 114 usando una tarjeta inteligente 116. A continuación, en el bloque de función 350 el HSM 114 genera un bloque de PIN usando el PIN cifrado.

La interfaz de HSM 110 envía el bloque de PIN generado al gestor de transacciones en el bloque de función 352. El gestor de transacciones 102 genera un mensaje de transacción usando los datos de transacción y el bloque de PIN en el bloque de función 354. A continuación, el gestor de transacciones 102 envía el mensaje de transacción a la Red de ATM 118 en el bloque de función 356. La Red de ATM 118 envía una solicitud de autorización a la Entidad Financiera 120 en el bloque de función 358.

En el bloque de decisión 360, la entidad financiera 120 determina si la transacción está autorizada. Si la transacción no está autorizada, el proceso sigue la ruta NO hacia el bloque de función 362 en donde la entidad financiera 120 envía un mensaje de “transacción denegada” al sector de transacciones 102. El gestor de transacciones 102 envía un mensaje de “transacción denegada” al servidor de comercio 108 en el bloque de función 364. El proceso finaliza en el bloque 500.

Si la transacción se autoriza, el proceso sigue la ruta SÍ hacia el bloque de función 366. La entidad financiera 120 envía un mensaje de “transacción aprobada” al gestor de transacciones en el bloque de función 366. El gestor de transacciones 102 envía un mensaje de “transacción aprobada” al servidor de comercio 108. La entidad financiera 120 efectúa un cargo en la cuenta del cliente de acuerdo con los datos de transacción en el bloque de función 370. El proceso finaliza en el bloque 500.

Aquellos expertos en la materia que disfruten del beneficio de la presente exposición apreciarán que esta invención proporciona un sistema y un método de procesado seguro de PIN. Debería entenderse que los dibujos y la descripción detallada de la presente deben considerarse con carácter ilustrativo y no restrictivo, y no están destinados a limitar la invención a las formas y ejemplos particulares dados a conocer. Por el contrario, la invención incluye cualesquiera modificaciones, cambios, redistribuciones, sustituciones, alternativas, elecciones de diseño, y formas de realización adicionales y evidentes para aquellos con conocimientos habituales en la materia, sin desviarse con respecto al espíritu y el alcance de esta invención, según definen las siguientes reivindicaciones. Así, se pretende que las siguientes reivindicaciones se interpreten de manera que abarcan todas estas modificaciones, cambios, redistribuciones, sustituciones, alternativas, elecciones de diseño, y formas de realización adicionales.

REIVINDICACIONES

1. Método de procesado seguro de números de identificación personal (PIN) en una transacción en red entre un terminal (104) y un servidor de comercio (108), en el que el servidor de comercio (108) establece una conexión de red entre el terminal (104) y un gestor de transacciones (102), de tal manera que el servidor de comercio (108) no tenga conocimiento de los datos intercambiados entre el terminal (104) y el gestor de transacciones (102), comprendiendo el método las etapas siguientes:

generar unos datos de terminal que definen un secreto no compartido, por medio de un gestor de transacciones (102);

generar unos datos de módulo de seguridad de hardware (HSM) que definen un secreto no compartido, por medio del gestor de transacciones (102);

enviar datos de terminal desde el gestor de transacciones (102) a un terminal (104);

en el que el terminal (104) genera una interfaz gráfica de introducción de PIN que comprende un teclado usando el secreto no compartido definido por los datos de terminal, graba los datos de posición del cursor que indican posiciones de cursor de un cursor de ratón del terminal (104) cuando el cursor del ratón se usa para seleccionar dígitos de un PIN por medio de la interfaz gráfica de introducción de PIN, genera los datos corolarios en relación con el PIN usando el secreto no compartido definido por los datos de terminal y los datos de posición del cursor, siendo el teclado aleatorizado, de tal manera que una posición dada del cursor del ratón indique un numeral diferente con cada dígito introducido;

recibir en el gestor de transacciones (102) los datos corolarios desde dicho terminal (104);

enviar los datos corolarios y los datos de módulo de seguridad de hardware (HSM) desde el gestor de transacciones (102) a un módulo de seguridad de hardware (114);

en el que el módulo de seguridad de hardware (114) calcula el PIN basándose en los datos corolarios y los datos de HSM, y en el que el módulo de seguridad de hardware (114) cifra el PIN y genera un bloque de PIN que incluye el PIN cifrado;

recibir en el gestor de transacciones (102) el bloque de PIN desde dicho módulo de seguridad de hardware (114), generar por medio del gestor de transacciones (102) una solicitud de transacción que incluye dicho bloque de PIN y transmitir dicha solicitud de transacción desde el gestor de transacciones (102) para la autenticación del PIN y la transacción;

determinar en el gestor de transacciones (102) si una entidad financiera (120) ha autenticado la transacción; y

notificar al servidor de comercio, por medio del gestor de transacciones (102), si se ha autenticado la transacción basándose en la etapa de determinación.

2. Método según la reivindicación 1, en el que dichos datos de terminal incluyen algoritmos.

3. Método según la reivindicación 1, en el que dichos datos de terminal incluyen datos semilla.

4. Método según la reivindicación 1, que comprende además la etapa de recibir datos de transacción desde el terminal e incluir dichos datos de transacción en dicha solicitud de transacción.

5. Sistema para el procesado seguro de números de identificación personal (PIN), que comprende:

un gestor de transacciones (102) para gestionar una transacción entre un terminal (104) y un servidor de comercio (108), generando el gestor de transacciones (102) datos de terminal que definen un secreto no compartido, y generando el gestor de transacciones (102) datos de módulo de seguridad de hardware (HSM) que definen un secreto no compartido;

un módulo de transacciones ejecutado por el terminal (104) y conectado con capacidad de comunicación a dicho gestor de transacciones (102) para recibir los datos de terminal desde el gestor de transacciones (102), generar una interfaz gráfica de introducción de PIN que comprende un teclado usando el secreto no compartido definido por los datos de terminal, grabar los datos de posición de cursor que indican posiciones de cursor de un cursor de ratón del terminal (104) cuando el cursor del ratón se usa para seleccionar dígitos de un PIN por medio de la interfaz gráfica de introducción de PIN, generar los datos corolarios en relación con el PIN usando el secreto no compartido definido por los datos de terminal y los datos de posición del cursor, y enviar los datos corolarios al gestor de transacciones (102), no teniendo el servidor de comercio (108) conocimiento de los datos intercambiados entre el terminal (104) y el gestor de transacciones (102), basándose los datos de entrada del

usuario en entradas del usuario recibidas por el terminal (104), y siendo el teclado aleatorizado, de tal manera que una posición dada del cursor del ratón indique un numeral diferente con cada dígito introducido;

y un módulo de seguridad de hardware (114) conectado con capacidad de comunicación a dicho gestor de transacciones (102), para recibir los datos corolarios y los datos de HSM desde el gestor de transacciones (102), calcular el PIN basándose en los datos corolarios y los datos de HSM, cifrar el PIN y generar un bloque de PIN que incluye el PIN cifrado; recibiendo dicho gestor de transacciones (102) el bloque de PIN desde dicho módulo de seguridad de hardware (114); genera una solicitud de transacción que incluye dicho bloque de PIN, transmite dicha solicitud de transacción para la autenticación del PIN y la transacción, determina si una entidad financiera (120) ha autenticado la transacción, y notifica al servidor de comercio (108) si la transacción ha sido autenticada.

6. Sistema de la reivindicación 5, en el que dicho gestor de transacciones está conectado con capacidad de comunicación a dicho módulo de transacciones por una red abierta.

7. Sistema de la reivindicación 5, en el que dicho gestor de transacciones está conectado con capacidad de comunicación a dicho módulo de seguridad de hardware por una conexión directa.

8. Sistema de la reivindicación 5, en el que dichos datos de terminal incluyen un algoritmo.

9. Sistema de la reivindicación 5, en el que dichos datos de HSM incluyen un algoritmo.

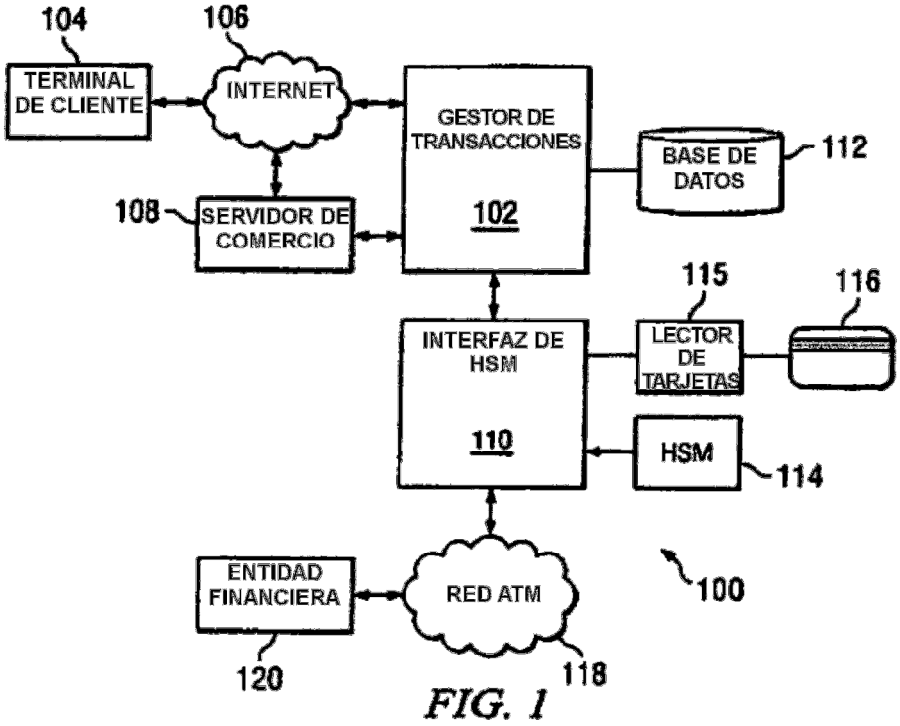

104
106
TERMINAL DE CLIENTE
INTERNET
GESTOR DE TRANSACCIONES
102
BASE DE DATOS
112
108
SERVIDOR DE COMERCIO
115
116
INTERFAZ DE HSM
110
LECTOR DE TARJETAS
HSM
114
ENTIDAD FINANCIERA
RED ATM
100
120
118

FIG. 1

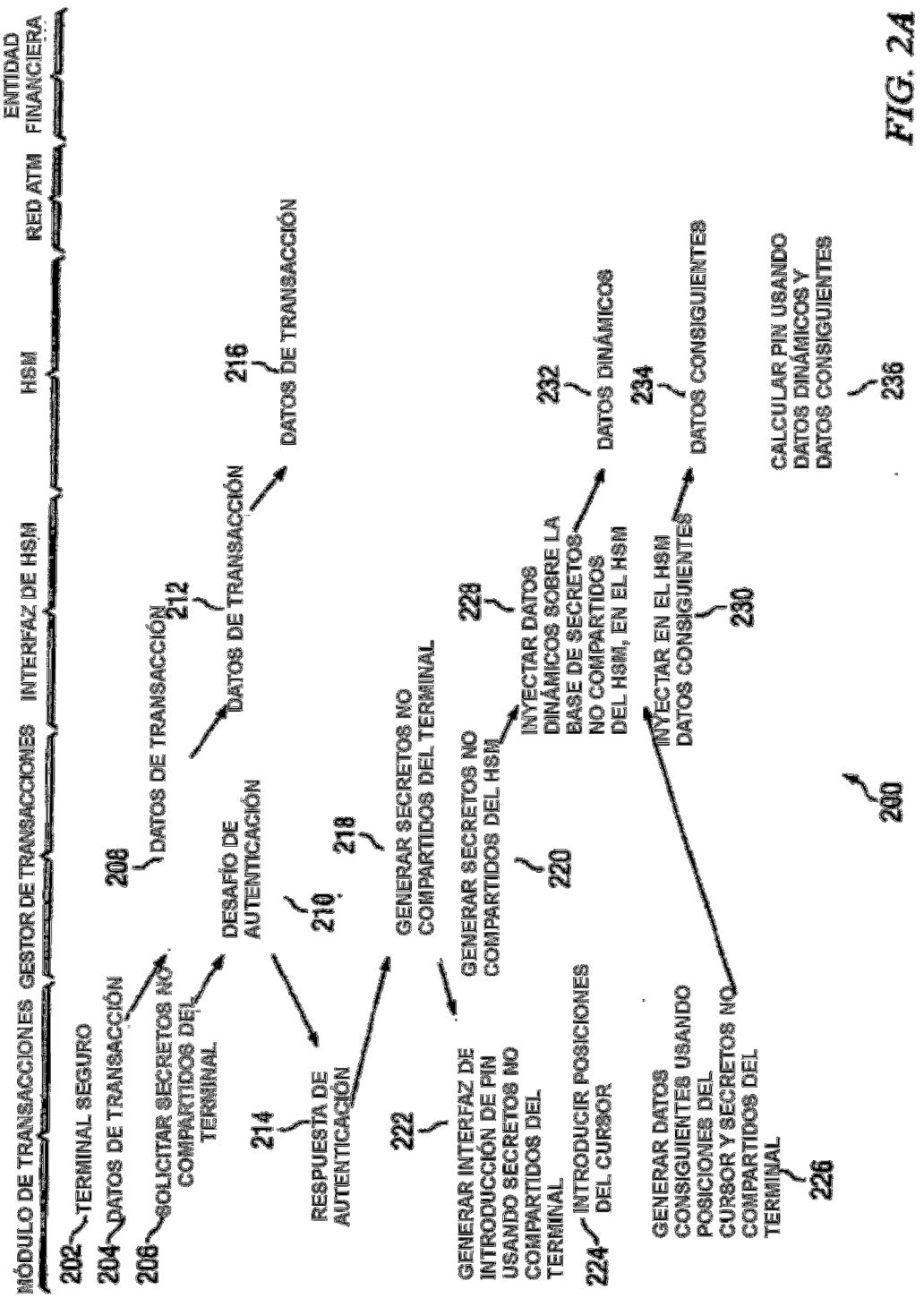

MÓDULO DE TRANSACCIONES
GESTOR DE TRANSACCIONES
INTERFAZ DE HSM
HSM
RED ATM
ENTIDAD FINANCIERA
202 TERMINAL SEGURO
204 DATOS DE TRANSACCIÓN
206 SOLICITAR SECRETOS NO COMPARTIDOS DEL TERMINAL
208 DATOS DE TRANSACCIÓN
212 DATOS DE TRANSACCIÓN
216 DATOS DE TRANSACCIÓN
DESAFÍO DE AUTENTICACIÓN
210
214 RESPUESTA DE AUTENTICACIÓN
218 GENERAR SECRETOS NO COMPARTIDOS DEL TERMINAL
222 GENERAR INTERFAZ DE INTRODUCCIÓN DE PIN USANDO SECRETOS NO COMPARTIDOS DEL TERMINAL
224 INTRODUCIR POSICIONES DEL CURSOR
220 GENERAR SECRETOS NO COMPARTIDOS DEL HSM
228 INYECTAR DATOS DINÁMICOS SOBRE LA BASE DE SECRETOS NO COMPARTIDOS DEL HSM, EN EL HSM
232 DATOS DINÁMICOS
234 DATOS CONSIGUIENTES
230 INYECTAR EN EL HSM DATOS CONSIGUIENTES
GENERAR DATOS CONSIGUIENTES USANDO POSICIONES DEL CURSOR Y SECRETOS NO COMPARTIDOS DEL TERMINAL
226
CALCULAR PIN USANDO DATOS DINÁMICOS Y DATOS CONSIGUIENTES
236
200

FIG. 2A

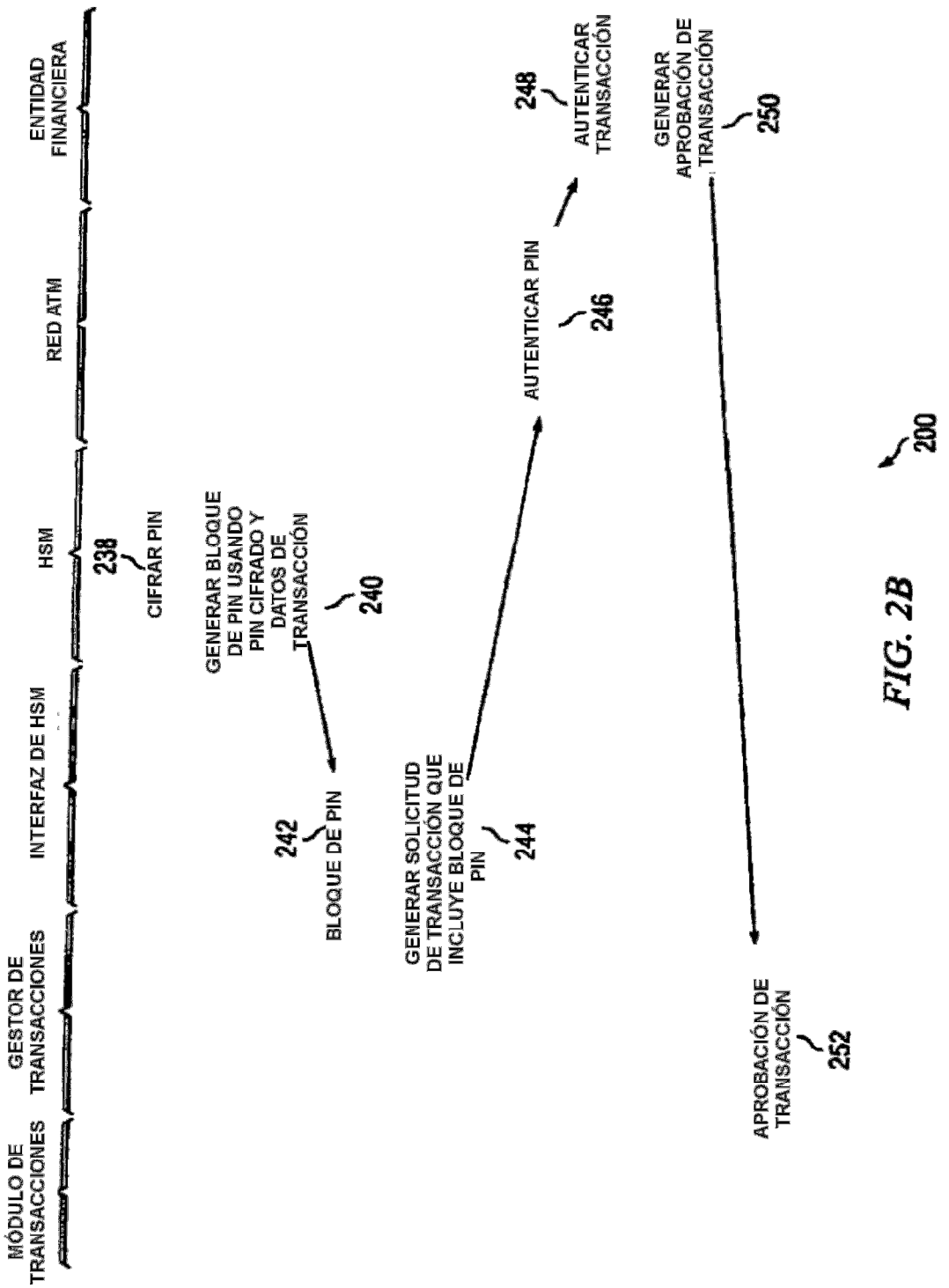
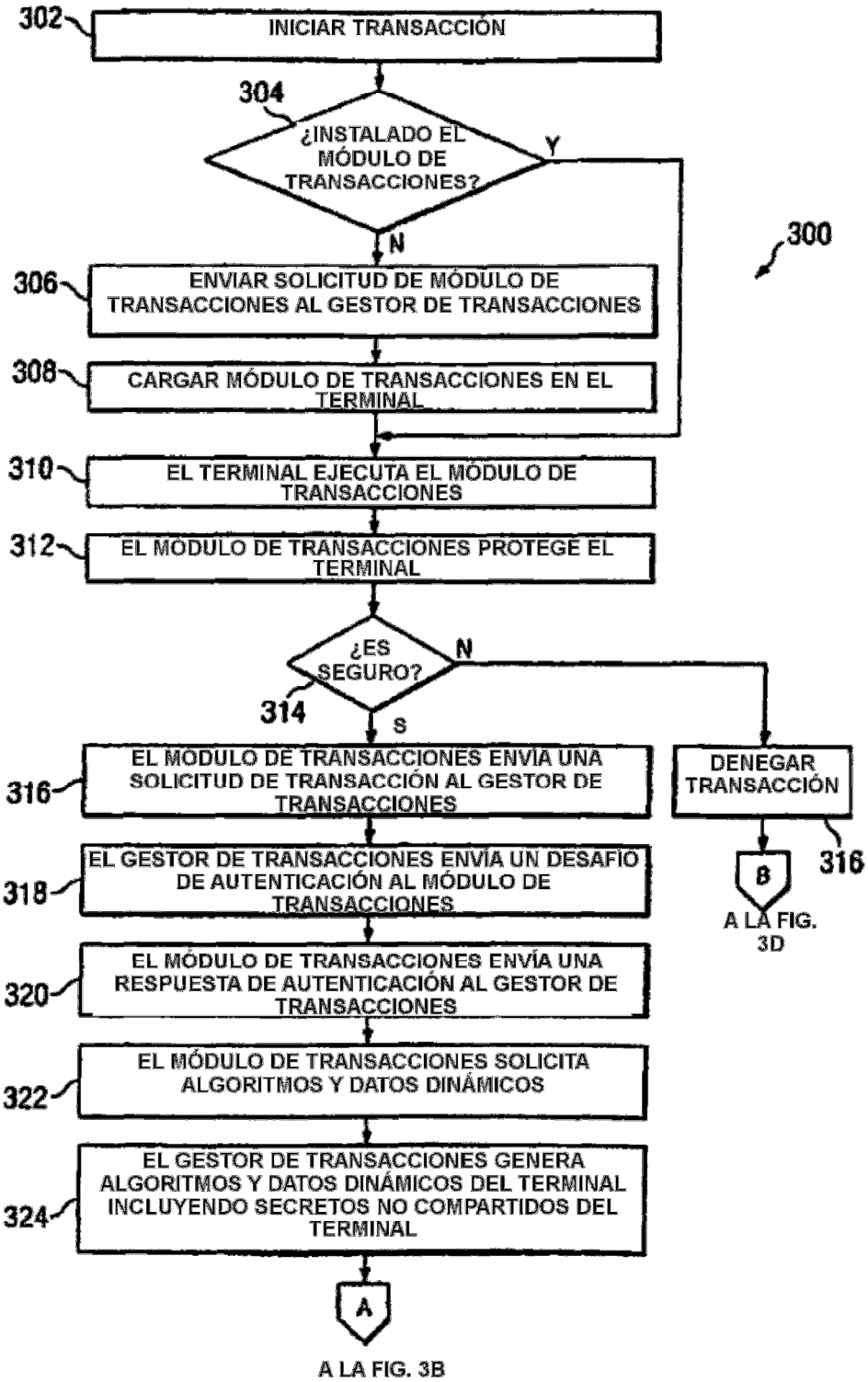
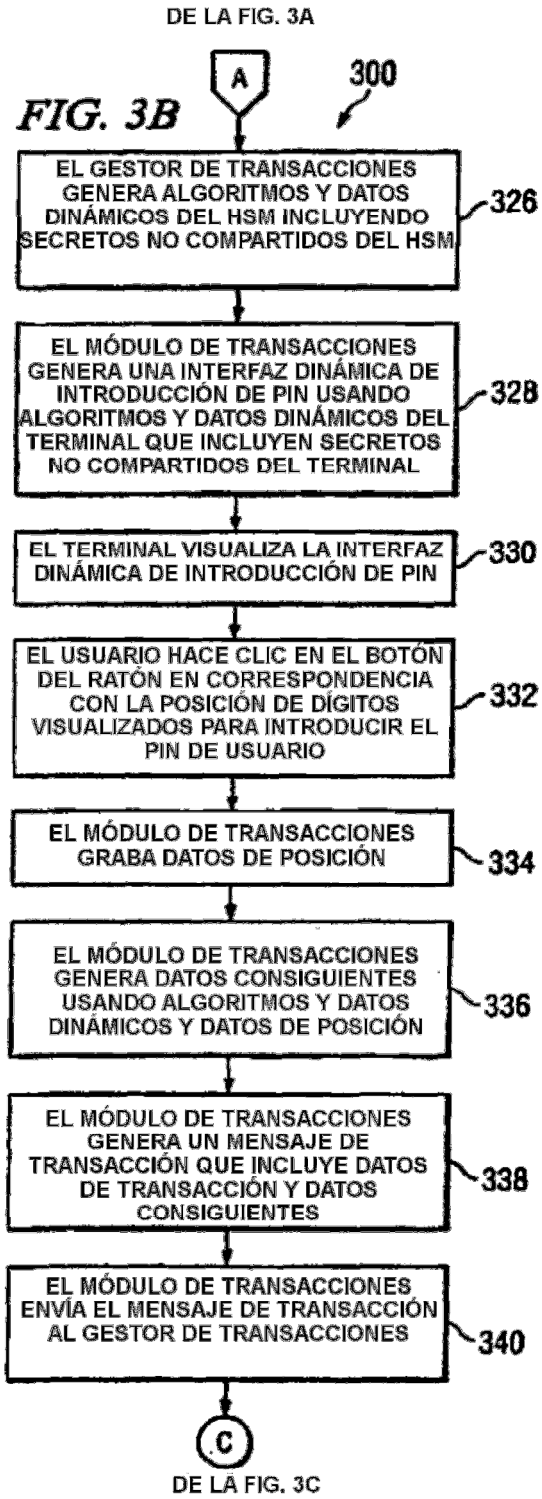
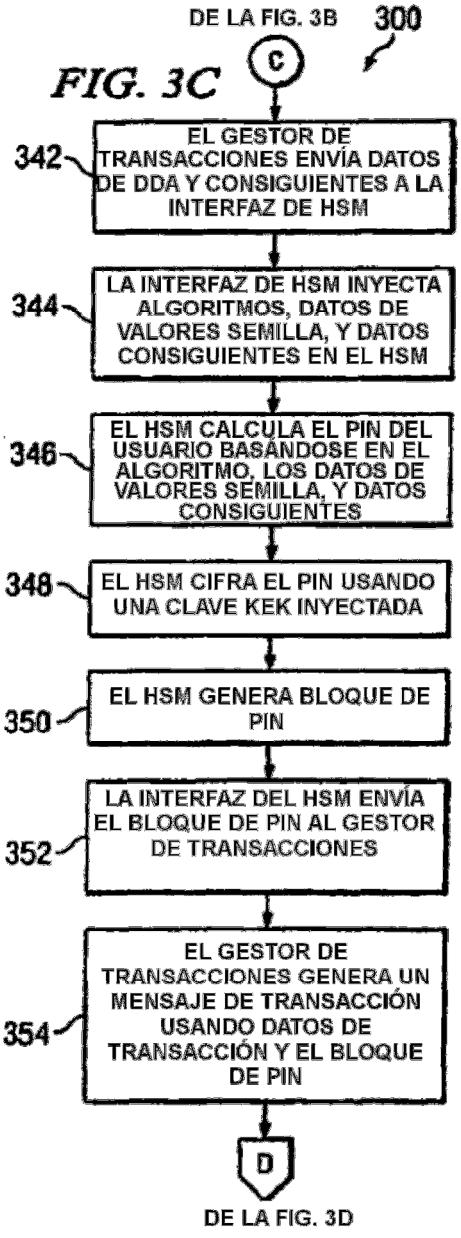

MÓDULO DE TRANSACCIONES
GESTOR DE TRANSACCIONES
INTERFAZ DE HSM
HSM
RED ATM
ENTIDAD FINANCIERA
238
CIFRAR PIN
GENERAR BLOQUE DE PIN USANDO PIN CIFRADO Y DATOS DE TRANSACCIÓN
240
242
BLOQUE DE PIN
GENERAR SOLICITUD DE TRANSACCIÓN QUE INCLUYE BLOQUE DE PIN
244
AUTENTICAR PIN
246
248
AUTENTICAR TRANSACCIÓN
GENERAR APROBACIÓN DE TRANSACCIÓN
250
APROBACIÓN DE TRANSACCIÓN
252
200

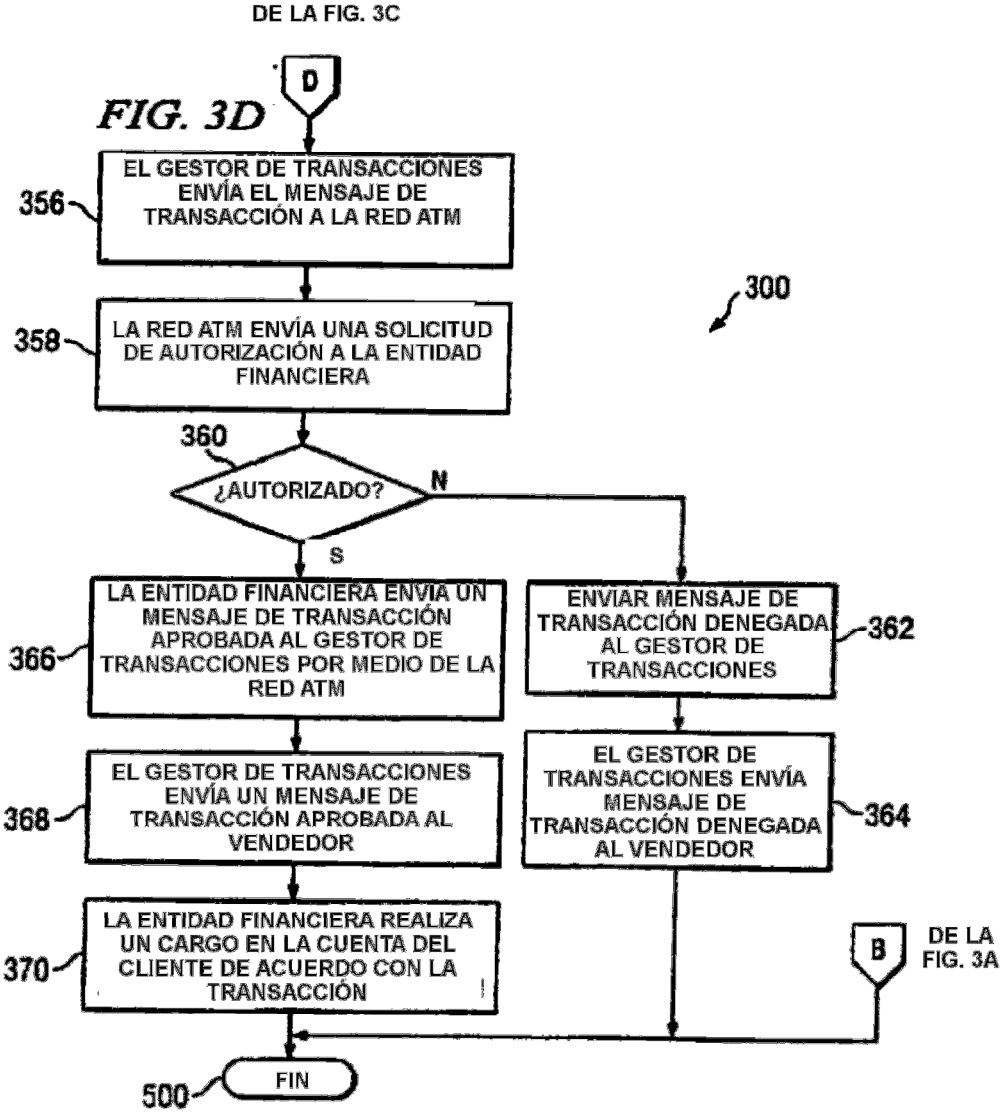
FIG. 2B

FIG. 3A


302
INICIAR TRANSACCIÓN
304
¿INSTALADO EL MÓDULO DE TRANSACCIONES?
Y
N
300
306
ENVIAR SOLICITUD DE MÓDULO DE TRANSACCIONES AL GESTOR DE TRANSACCIONES
308
CARGAR MÓDULO DE TRANSACCIONES EN EL TERMINAL
310
EL TERMINAL EJECUTA EL MÓDULO DE TRANSACCIONES
312
EL MÓDULO DE TRANSACCIONES PROTEGE EL TERMINAL
¿ES SEGURO?
314
N
S
316
EL MÓDULO DE TRANSACCIONES ENVÍA UNA SOLICITUD DE TRANSACCIÓN AL GESTOR DE TRANSACCIONES
DENEGAR TRANSACCIÓN
316
B
A LA FIG. 3D
318
EL GESTOR DE TRANSACCIONES ENVÍA UN DESAFÍO DE AUTENTICACIÓN AL MÓDULO DE TRANSACCIONES
320
EL MÓDULO DE TRANSACCIONES ENVÍA UNA RESPUESTA DE AUTENTICACIÓN AL GESTOR DE TRANSACCIONES
322
EL MÓDULO DE TRANSACCIONES SOLICITA ALGORITMOS Y DATOS DINÁMICOS
324
EL GESTOR DE TRANSACCIONES GENERA ALGORITMOS Y DATOS DINÁMICOS DEL TERMINAL INCLUYENDO SECRETOS NO COMPARTIDOS DEL TERMINAL
A
A LA FIG. 3B


DE LA FIG. 3A
A
300
FIG. 3B
EL GESTOR DE TRANSACCIONES GENERA ALGORITMOS Y DATOS DINÁMICOS DEL HSM INCLUYENDO SECRETOS NO COMPARTIDOS DEL HSM
326
EL MÓDULO DE TRANSACCIONES GENERA UNA INTERFAZ DINÁMICA DE INTRODUCCIÓN DE PIN USANDO ALGORITMOS Y DATOS DINÁMICOS DEL TERMINAL QUE INCLUYEN SECRETOS NO COMPARTIDOS DEL TERMINAL
328
EL TERMINAL VISUALIZA LA INTERFAZ DINÁMICA DE INTRODUCCIÓN DE PIN
330
EL USUARIO HACE CLIC EN EL BOTÓN DEL RATÓN EN CORRESPONDENCIA CON LA POSICIÓN DE DÍGITOS VISUALIZADOS PARA INTRODUCIR EL PIN DE USUARIO
332
EL MÓDULO DE TRANSACCIONES GRABA DATOS DE POSICIÓN
334
EL MÓDULO DE TRANSACCIONES GENERA DATOS CONSIGUIENTES USANDO ALGORITMOS Y DATOS DINÁMICOS Y DATOS DE POSICIÓN
336
EL MÓDULO DE TRANSACCIONES GENERA UN MENSAJE DE TRANSACCIÓN QUE INCLUYE DATOS DE TRANSACCIÓN Y DATOS CONSIGUIENTES
338
EL MÓDULO DE TRANSACCIONES ENVÍA EL MENSAJE DE TRANSACCIÓN AL GESTOR DE TRANSACCIONES
340
C
DE LA FIG. 3C


DE LA FIG. 3B
300
C
FIG. 3C
342
EL GESTOR DE TRANSACCIONES ENVÍA DATOS DE DDA Y CONSIGUIENTES A LA INTERFAZ DE HSM
344
LA INTERFAZ DE HSM INYECTA ALGORITMOS, DATOS DE VALORES SEMILLA, Y DATOS CONSIGUIENTES EN EL HSM
346
EL HSM CALCULA EL PIN DEL USUARIO BASÁNDOSE EN EL ALGORITMO, LOS DATOS DE VALORES SEMILLA, Y DATOS CONSIGUIENTES
348
EL HSM CIFRA EL PIN USANDO UNA CLAVE KEK INYECTADA
350
EL HSM GENERA BLOQUE DE PIN
352
LA INTERFAZ DEL HSM ENVÍA EL BLOQUE DE PIN AL GESTOR DE TRANSACCIONES
354
EL GESTOR DE TRANSACCIONES GENERA UN MENSAJE DE TRANSACCIÓN USANDO DATOS DE TRANSACCIÓN Y EL BLOQUE DE PIN
D
DE LA FIG. 3D


DE LA FIG. 3C
D
FIG. 3D
EL GESTOR DE TRANSACCIONES ENVÍA EL MENSAJE DE TRANSACCIÓN A LA RED ATM
356
LA RED ATM ENVÍA UNA SOLICITUD DE AUTORIZACIÓN A LA ENTIDAD FINANCIERA
358
300
360
¿AUTORIZADO?
N
S
LA ENTIDAD FINANCIERA ENVIA UN MENSAJE DE TRANSACCIÓN APROBADA AL GESTOR DE TRANSACCIONES POR MEDIO DE LA RED ATM
366
ENVIAR MENSAJE DE TRANSACCIÓN DENEGADA AL GESTOR DE TRANSACCIONES
362
EL GESTOR DE TRANSACCIONES ENVÍA UN MENSAJE DE TRANSACCIÓN APROBADA AL VENDEDOR
368
EL GESTOR DE TRANSACCIONES ENVÍA MENSAJE DE TRANSACCIÓN DENEGADA AL VENDEDOR
364
LA ENTIDAD FINANCIERA REALIZA UN CARGO EN LA CUENTA DEL CLIENTE DE ACUERDO CON LA TRANSACCIÓN
370
B
DE LA FIG. 3A
FIN
500