(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 748 847**

(51) Int. CI.:

G06Q 40/00 (2012.01)
G06Q 20/00 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.05.2008 PCT/US2008/063966**

(87) Fecha y número de publicación internacional: **27.11.2008 WO08144555**

(96) Fecha de presentación y número de la solicitud europea: **16.05.2008 E 08755755 (9)**

(97) Fecha y número de publicación de la concesión europea: **26.06.2019 EP 2156397**

(54) Título: **Transacciones de tarjeta de pago seguras**

(30) Prioridad:

17.05.2007 US 750239
17.05.2007 US 750181
17.05.2007 US 750184

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.03.2020

(73) Titular/es:

SHIFT4 CORPORATION (100.0%)
1491 Center Crossing Road
Las Vegas, NV 89144, US

(72) Inventor/es:

ODER, JOHN DAVID, II.;
ODER, JOHN DAVID;
CRONIC, KEVIN JAMES;
SOMMERS, STEVEN MARK y
WARNER, DENNIS WILLIAM

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Transacciones de tarjeta de pago seguras

Antecedentes

Campo

La presente divulgación se refiere a sistemas de pago.

Descripción de la técnica relacionada

El uso de tarjetas de pago tales como tarjetas de crédito, tarjetas de débito, y tarjetas de regalos se ha vuelto común en nuestra sociedad de transacciones comerciales actual. De manera virtual, cada comerciante, así como otras instalaciones donde tienen lugar transacciones monetarias para la compra de bienes o servicios, acepta uno o más tipos de tarjetas de pago para estas transacciones. Una vez que se presenta una tarjeta de pago a un comerciante particular en un punto de venta para comprar bienes o servicios, la tarjeta de pago se lee normalmente usando un lector de paso de tarjeta. Como alternativa, se introducen manualmente datos de pago a través de un teclado de pin o teclado o a través de una combinación de pasada de tarjeta y entrada manual.

Los datos de pago se transmiten a una entidad de autoridad, que puede ser un procesador de tarjeta, asociación de tarjeta, banco emisor, u otra entidad, junto con información relacionada con el precio de compra e información de identificación del comerciante particular. En algunos casos, la información pasa a través de uno o más intermediarios antes de alcanzar la entidad de autorización. La entidad de autorización aprueba o desaprueba la transacción. Una vez que se realiza una decisión en la entidad de autorización, se envía un mensaje de retorno al comerciante que indica la disposición de la transacción.

A medida que las transacciones de tarjeta de pago se hacen más comunes, también lo hacen los robos de datos de pago. Los robos pueden provenir de muchas fuentes, incluyendo empleados, software malicioso y dispositivos de hardware para interceptar datos de pago. Los perpetradores obtienen datos de pago, que incluyen números de cuenta personal (PAN), números de identificación personal (PIN), fechas de caducidad y similares, para los fines de cometer fraude. En algunos casos, los ladrones usan los datos de pago para obtener bienes, servicios y efectivo. En otras instancias, los perpetradores venden datos de pago a otros que usan de manera fraudulenta las tarjetas. Estos robos a menudo tienen lugar en el punto de venta.

El documento EP1324564A2 describe un sistema y método para asegurar datos transaccionales comunicados a través de una red inalámbrica en una tienda minorista ofuscando mensajes de transacción en un flujo de tráfico. El sistema incluye un equilibrador de carga acoplado a un anfitrión y una pluralidad de terminales conectados al anfitrión a través de una red inalámbrica. El equilibrador de carga determina periodos de tiempo en espera de la comunicación. Si este tiempo es mayor que un umbral, se envía un mensaje de solicitud de transacción falso a uno o más terminales. Por consiguiente, los mensajes de transacción falsos con datos de cliente, cuenta y de transacción falsos se transmiten por los terminales al anfitrión hasta que se agota un temporizador o comienza una transacción real. Los mensajes de transacción reales y falsos también están encriptados para aumentar el tiempo de procesamiento para los mensajes por los espías.

El documento WO0129637A2 describe un sistema y método para realizar transacciones electrónicas seguras. Se desvela un sistema de servidor central que puede procesar y correlacionar números o datos de intermediario que se sustituyen para datos personales e información financiera durante transacciones donde la información podría interceptarse o usarse incorrectamente por el receptor. En el modo preferido, se usan números de transacción por clientes para encubrir su número de tarjeta de crédito real de comerciantes en línea y aquellos que intentarían interceptar números de tarjeta de crédito usados en transacciones en línea.

El documento US2005177442A1 describe un método y sistema para realizar transacciones minoristas que permite el uso de un dispositivo inalámbrico en lugar de tarjetas financieras convencionales. Un sistema minorista envía datos de transacción independientes de cliente, que se hacen coincidir con una cuenta de cliente asociada con un dispositivo inalámbrico. Un cliente envía una comunicación inalámbrica de un dispositivo inalámbrico a un servidor. El servidor identifica el dispositivo inalámbrico e identifica una cuenta de cliente asociada con el dispositivo inalámbrico. La cuenta de cliente y los datos de transacción independientes del cliente se hacen coincidir juntos, autorizando la transacción minorista. Cuando tienen lugar múltiples transacciones minoristas en un breve tiempo, una técnica de coincidencia hace coincidir entre múltiples transacciones minoristas y múltiples comunicaciones inalámbricas iniciadas por el cliente.

El documento US2001021925A1 describe un dispositivo de agente conectado a un dispositivo de usuario para explorar un sitio de comerciante, para vender productos en línea y ser servido en la Internet, el sitio de comerciante, y un dispositivo de servidor de una compañía de tarjeta de crédito. En el caso donde se emita una instrucción de compra de un producto explorado por el dispositivo de usuario, la instrucción se envía al dispositivo de agente. El dispositivo

de agente extrae un número de tarjeta de crédito de una tarjeta de crédito mantenida por un usuario que ha comprado el producto, y consulta al dispositivo de servidor de la compañía de la tarjeta de crédito si el producto ha de comprarse con la tarjeta de crédito. Como un resultado de la consulta, en el caso donde el producto pueda comprarse en línea con la tarjeta de crédito, el dispositivo de agente envía una instrucción de que el usuario compra el producto en línea con la tarjeta de crédito.

El documento US6000832A describe un sistema de comercio en línea que facilita el comercio en línea a través de una red pública usando una tarjeta de comercio en línea. La "tarjeta" no existe en forma física, sino que en su lugar existe en forma digital. Se asigna a un número de cuenta de cliente que incluye dígitos para un número de prefijo para información de manejo de banco, dígitos para un número de identificación de cliente, dígitos reservados para un número de código embebido y un dígito para suma de comprobación. El banco también proporciona al cliente una clave privada. Durante una transacción en línea, el ordenador de cliente recupera la clave privada y la cuenta de cliente a partir del almacenamiento. El ordenador de cliente genera un número de código como una función de la clave privada, datos específicos de cliente (por ejemplo, nombre del titular de la tarjeta, número de cuenta, etc.) y datos específicos de transacción (por ejemplo, cuenta de transacción, ID de comerciante, ID de bienes, tiempo, fecha de transacción, etc.). El ordenador de cliente embebe el número de código en los dígitos reservados del número de cuenta de cliente para crear un número de transacción específico a la transacción. El cliente emite ese número de transacción al cliente como un intermediario para un número de tarjeta regular. Cuando el comerciante emite el número para aprobación, la institución emisora lo reconoce como un número de transacción de intermediario, indexa el registro de cuenta de cliente, y busca la clave privada asociada y datos específicos de cliente. La institución calcula un número de código de prueba que usa la misma función y parámetros de entrada que el ordenador de cliente. La institución emisora compara el número de código de prueba con el número de código embebido en el número de transacción. Si los dos números coinciden, la institución de emisión acepta el número de transacción como válida.

El documento US2006261159A1 describe sistemas y métodos para monitorizar datos de transacción en un sistema de punto de venta (POS). Un componente en línea está conectado entre un terminal de POS y una impresora. El componente en línea monitoriza comunicaciones entre el terminal de POS y la impresora así como comunicaciones enviadas a o desde otros dispositivos conectados con el terminal de POS. A medida que se monitorizan los datos en las comunicaciones, se extraen porciones de los datos y se envían a un servidor de procesamiento remoto. El procesamiento remoto devuelve información que podría comprender una diversidad de información, tal como: datos disuasorios de fraude, promociones de tienda, mensajes de cliente y similares al componente en línea. El componente en línea envía esta información a la impresora para su presentación al usuario. La información se envía típicamente a la impresora sin interferir con la transacción que se está realizando por el terminal de POS. Los comandos incluidos en la información pueden implementarse por el componente en línea.

El documento US2005177521A1 describe un método para obtener una aprobación de un fichero de desembolso de transferencia electrónica de fondos (EFT) de un usuario de un sistema remoto y transferir el fichero de desembolso de EFT a un procesador de pagos. El método comprende generar un resumen, realizando una función de troceo del fichero de desembolso de EFT, y transferir el fichero al sistema remoto junto con código de control de autorización. El código de control de autorización controla el sistema remoto para obtener una firma digital de atributos autenticados, que incluye el resumen, y genera una respuesta de autorización. El método comprende adicionalmente recibir la respuesta de autorización del sistema remoto y transferir una presentación de fondos electrónica al procesador de pagos. La presentación de fondos electrónica comprende el fichero de transacción de pago y al menos una porción de la respuesta de autorización que comprende la firma digital.

El documento US2006036541A1 describe un sistema para procesar transacciones de pago de tarjeta de crédito iniciadas por un comerciante que incluye una interfaz para recibir una solicitud iniciada por el comerciante para una transferencia de fondos de una cuenta de tarjeta de crédito de comprador. Una aplicación de procesamiento de tarjeta de crédito inicia la transferencia de fondos de la cuenta de tarjeta de crédito del comprador a una cuenta bancaria de comerciante de terceros, mantenida por un servicio de pago de terceros. La cuenta bancaria de comerciante de terceros recibe fondos de la cuenta de tarjeta de crédito del comprador en nombre del comerciante. Una aplicación de asignación de fondos asigna los fondos recibidos a una cuenta de recepción del comerciante, manteniéndose la cuenta de recepción por el servicio de pago de terceros. La aplicación de procesamiento de tarjeta de crédito puede ser la aplicación de terminal de punto de venta (POS) virtual, alojada en un sistema informático de servidor operado por el servicio de pago de terceros, y en consecuencia puede ser accesible por el comerciante mediante una red.

El documento US2005204172A1 describe un sistema de gestión de información que comprende una o más estaciones de trabajo que ejecutan aplicaciones para permitir que un usuario de la estación de trabajo se conecte a una red, tal como Internet. Cada aplicación tiene un analizador, que monitoriza datos de transmisión que la aplicación está apunto de transmitir a la red o a punto de recibir de la red y que determina que se haga una acción apropiada con respecto a esos datos de transmisión. Tales acciones pueden ser extraer datos de los datos de transmisión, tales como contraseñas y nombres de usuario, certificados digitales o detalles de transacciones de comercio electrónico para su almacenamiento en una base de datos; asegurar que los datos de transmisión se transmiten en una fortaleza de encriptación apropiada a los contenidos de los datos de transmisión; determinar si necesita realizarse una comprobación en cuanto a si está en vigor un certificado digital recibido en los datos de transmisión, y determinar si una transacción que está a punto de hacerse por un usuario de una de las estaciones de trabajo necesita aprobación

de terceros. El analizador puede consultar unos datos de política que contienen una política para regir las estaciones de trabajo para hacer su determinación. El sistema de gestión de información proporciona muchas ventajas en el entorno de comercio electrónico a compañías de comercio en línea, que pueden beneficiarse pudiendo regular las transacciones realizadas por su personal de acuerdo con sus instrucciones en unos datos de política, mantener automáticamente registros de contraseñas y negocios realizados en línea, evitar pagar comprobaciones innecesarias sobre la validez de certificados digitales y asegurar que las transmisiones de datos realizadas por su personal se protegen siempre a una intensidad de encriptación acordada.

El documento US2003126094A1 describe métodos en línea, sistemas, y software para mejorar el procesamiento de pagos de cuentas financieras, particularmente pagos de tarjeta de crédito y débito realizados de consumidores a comerciantes en transacciones en línea. La realización preferida de la invención implica insertar un servicio en línea de terceros confiable en el proceso de autorización de pago. El tercero confiable autentica el cliente y autoriza al pago propuesto en un único proceso integrado realizado sin la implicación del comerciante. La autenticación del cliente se consigue a través de un canal de comunicación persistente establecido con el cliente antes de que se haga una compra. La autenticación se hace verificando que el canal persistente está abierto cuando se solicita la autorización. El uso de los servicios de terceros permite que el cliente evite revelar su identidad y número de tarjeta de crédito al comerciante a través de una red pública tal como Internet, mientras que mantiene el control de la transacción durante el proceso de autorización.

Sumario

Las realizaciones de la presente invención se definen en las reivindicaciones adjuntas 1-8.

Las transacciones de tarjeta de pago en un punto de venta (POS) pueden asegurarse interceptando, con una capa de seguridad de POS instalada en un terminal de POS, datos de pago del terminal de POS, transmitiendo los datos de pago de la capa de seguridad de POS a una aplicación de seguridad de servidor instalada en un servidor de POS, y proporcionando datos de pago falsos de la capa de seguridad de POS a una aplicación de terminal de POS instalada en el terminal de POS. Los datos de pago falsos en diversas realizaciones se procesan como si fueran los datos de pago, de manera que el terminal de POS transmite una solicitud de autorización al servidor de POS usando los datos de pago falsos. Además, la solicitud de autorización puede transmitirse del servidor de POS a una pasarela de pago.

También se proporciona un método para añadir seguridad a un terminal de punto de venta (POS) que comunica a través de una red con un servidor de POS, donde el terminal de POS puede incluir una aplicación de terminal de POS instalada en el mismo y un lector de tarjeta de pago, donde la aplicación de terminal de POS puede comunicar con el servidor de POS a través de un canal no seguro para procesar transacciones de tarjeta de pago. El método puede incluir instalar una capa de seguridad de POS en el terminal de POS, donde la capa de seguridad de POS puede al menos: (a) interceptar datos de pago recibidos del lector de tarjeta de pago cuando un usuario inicia una transacción de tarjeta de pago, donde los datos de pago incluyen datos de tarjeta reales, (b) pasar datos de tarjeta falsos a la aplicación de terminal de POS para su uso en lugar de los datos de tarjeta reales, de manera que los datos de tarjeta falsos se transmiten a través del canal no seguro al servidor de POS en lugar de los datos de tarjeta reales, y (c) transmitir los datos de tarjeta reales al servidor de POS a través de un canal seguro, de manera que se inhibe que se transmitan los datos de tarjeta reales a través de un canal no seguro.

En ciertos ejemplos, los datos de tarjeta falsos incluyen un número de tarjeta de pago falso. En ciertos ejemplos, los datos de tarjeta falsos se usan como si fueran los datos de tarjeta reales pero no corresponden a una cuenta de tarjeta de pago válida. En ciertas realizaciones, la capa de seguridad de POS genera al menos una porción de los datos de tarjeta falsos. En ciertos ejemplos, al menos se reutiliza una porción de los datos de tarjeta falsos como un testigo para transacción de tarjeta de pago adicional. En ciertos ejemplos, la capa de seguridad de POS visualiza una pantalla de pago sustituta que posibilita que un titular proporcione al menos una porción de los datos de pago a la capa de seguridad de POS. En ciertos ejemplos, los datos de tarjeta reales se obtienen de una pasada de tarjeta. En ciertas realizaciones, los datos de tarjeta reales se introducen manualmente.

También se proporciona un medio legible por ordenador que tiene almacenado en el mismo una capa de seguridad de POS que puede instalarse en un terminal de POS que ejecuta una aplicación de terminal de POS y que comunica con un servidor de POS a través de una red. La capa de seguridad de POS puede incluir instrucciones ejecutables que provocan al terminal de POS al menos: interceptar datos de pago reales recibidos de un dispositivo de entrada de tarjeta cuando un usuario inicia una transacción de tarjeta de pago, de manera que los datos de pago reales no se hacen disponibles a la aplicación de terminal de POS, pasar datos de pago falsos a la aplicación de terminal de POS para su uso en lugar de los datos de pago reales, de manera que la aplicación de terminal de POS transmite los datos de pago falsos al servidor de POS en lugar de los datos de pago reales, y transmitir los datos de pago reales al servidor de POS.

En ciertas realizaciones, la capa de seguridad de POS obtiene al menos una porción de los datos de pago falsos de una aplicación de seguridad que se ejecuta en el servidor de POS. En ciertas realizaciones, se generan los datos de pago falsos usando un algoritmo que garantiza sustancialmente que los datos de pago falsos no representan datos de tarjeta válidos. En ciertos ejemplos, la capa de seguridad de POS intercepta los datos de pago reales actuando como

un registrador de teclas. En ciertos ejemplos, la capa de seguridad de POS intercepta los datos de pago reales accediendo a una memoria intermedia de entrada en el terminal de POS. En ciertas realizaciones, los datos de pago falsos incluyen una porción de los datos de pago reales. En ciertas realizaciones, la capa de seguridad de POS encripta los datos de pago reales en el terminal de POS. En ciertas realizaciones, la capa de seguridad de POS proporciona seguridad a un terminal de POS no seguro preexistente. En ciertos ejemplos, la capa de seguridad de POS puede invocarse directamente por una acción de usuario. En ciertos ejemplos, la acción de usuario incluye una presión de tecla de acceso rápido o entrada de tarjeta de tecla manual. En ciertas realizaciones, la capa de seguridad de POS puede invocarse indirectamente mediante la entrada de los datos de pago en el terminal de POS. En ciertos ejemplos, la capa de seguridad de POS puede invocarse por programación. En ciertos ejemplos, los datos de pago reales se transmiten al servidor de POS a través de un canal seguro.

Un método de aseguración de transacciones de pago en un POS incluye interceptar datos de pago en un terminal de POS, donde los datos de pago incluyen datos de pago reales de un medio de pago, y proporcionar datos de pago falsos al terminal de POS, los datos de pago falsos procesados como si fueran los datos de pago reales, de manera que el terminal de POS transmite una solicitud de autorización usando los datos de pago falsos en lugar de los datos de pago reales.

Se proporciona un método para proporcionar datos de pago falsos para su uso en lugar de datos de pago reales en un POS para inhibir la transmisión de datos de pago reales a través de un canal no seguro. El método puede incluir capturar datos de pago en un terminal de POS, donde los datos de pago incluyen datos de tarjeta reales de una tarjeta de pago, generar datos de tarjeta falsos que pueden procesarse como si fueran los datos de tarjeta reales, donde los datos de tarjeta falsos pueden configurarse de manera que una prueba de módulo 10 de Luhn realizada en los datos de tarjeta falsos determina que los datos de tarjeta falsos incluyen un número de tarjeta de pago inválido, y proporcionar los datos de tarjeta falsos al terminal de POS, de manera que el terminal de POS transmite una solicitud de autorización al servidor de POS usando los datos de tarjeta falsos en lugar de los datos de tarjeta reales.

Se proporciona un método para añadir seguridad a un servidor de POS que comunica a través de una red con uno o más terminales de POS, donde cada terminal de POS incluye un lector de tarjeta de pago, donde el servidor de POS incluye una aplicación de servidor de POS instalada en el mismo que puede comunicar con el uno o más terminales de POS a través de un canal no seguro para procesar transacciones de tarjeta de pago. El método puede incluir instalar una aplicación de seguridad de servidor en el servidor de POS, donde la aplicación de seguridad de servidor puede al menos: (a) recibir datos de pago del uno o más terminales de POS a través de un canal seguro, los datos de pago incluyen datos de tarjeta reales obtenidos del lector de la tarjeta de pago, (b) proporcionar datos de tarjeta falsos al terminal de POS, los datos de tarjeta falsos configurados para procesarse como si fueran los datos de tarjeta reales, (c) recibir una primera solicitud de autorización del terminal de POS a través del canal no seguro, donde la primera solicitud de autorización puede incluir los datos de tarjeta falsos en lugar de los datos de tarjeta reales, y (d) transmitir una segunda solicitud de autorización a un servidor remoto, donde la segunda solicitud de autorización puede incluir al menos los datos de tarjeta reales.

Puede proporcionarse un medio legible por ordenador que tiene almacenado en el mismo una aplicación de seguridad de servidor que puede estar instalada en un servidor de POS que ejecuta una aplicación de servidor de POS y que comunica con un terminal de POS a través de una red. La aplicación de seguridad de servidor puede incluir instrucciones ejecutables que provocan al servidor de POS al menos: recibir datos de pago del terminal de POS, donde los datos de pago pueden incluir datos de tarjeta reales de una tarjeta de pago, recibir una primera solicitud de autorización del terminal de POS, donde la primera solicitud de autorización incluye datos de tarjeta falsos en lugar de los datos de tarjeta reales, donde los datos de tarjeta falsos se procesan como si fueran los datos de tarjeta reales, y transmitir una segunda solicitud de autorización, la segunda solicitud de autorización incluye al menos los datos de tarjeta reales.

Un método para asegurar transacciones de tarjeta de pago en un POS incluye recibir, en un servidor de POS, datos de pago de un terminal de POS, donde los datos de pago incluyen datos de pago reales de un medio de pago, y recibir, en el servidor de POS, una primera solicitud de autorización del terminal de POS, donde la primera solicitud de autorización incluye datos de pago falsos en lugar de los datos de pago reales, donde los datos de pago falsos pueden procesarse como si fueran los datos de pago reales.

Un método para asegurar transacciones de tarjeta de pago en una pasarela de pago puede incluir recibir, en una pasarela de pago, una solicitud de autorización de un servidor de POS, donde la solicitud de autorización puede incluir datos de pago y datos de tarjeta falsos combinados, donde los datos de pago pueden incluir datos de tarjeta reales de una tarjeta de pago, donde los datos de pago falsos pueden procesarse como si fueran los datos de pago, extraer los datos de pago de los datos de pago y datos de pago falsos combinados, transmitir una solicitud de autorización de la pasarela de pago a una entidad de autoridad, donde la solicitud de autorización incluye los datos de pago, recibir una respuesta a la solicitud de autorización de la entidad de autorización, y transmitir la respuesta y los datos de pago falsos al servidor de POS, donde los datos de pago falsos pueden identificar de manera inequívoca la al menos una tarjeta de pago.

Se proporciona un método para añadir seguridad a un sistema de POS que incluye un terminal de POS que comunica

a través de una red con un servidor de POS, donde el lector de terminal de POS incluye una tarjeta de pago y tiene una aplicación de terminal de POS instalada en el mismo, donde el servidor de POS tiene una aplicación de servidor de POS instalada en el mismo que comunica con la aplicación de terminal de POS a través de un canal no seguro para procesar transacciones de tarjeta de pago. El método puede incluir instalar una capa de seguridad de POS en el terminal de POS, donde la capa de seguridad de POS puede al menos (a) interceptar datos de tarjeta reales recibidos del lector de la tarjeta de pago cuando un usuario inicia una transacción de tarjeta de pago, (b) pasar datos de tarjeta falsos a la aplicación de terminal de POS para su uso en lugar de los datos de tarjeta reales, de manera que los datos de tarjeta falsos se transmiten a través del canal no seguro al servidor de POS en lugar de los datos de tarjeta reales, y (c) transmitir los datos de tarjeta reales al servidor de POS a través de un canal seguro. El método puede incluir adicionalmente instalar una aplicación de seguridad de servidor en el servidor de POS, donde la aplicación de seguridad de servidor puede recibir los datos de tarjeta reales de la capa de seguridad de POS a través del canal seguro y usar los datos de tarjeta falsos para procesar la transacción de tarjeta de pago.

Un método para asegurar transacciones de tarjeta de pago en un POS puede incluir interceptar, con una capa de seguridad de POS instalada en un terminal de POS, datos de pago del terminal de POS, donde los datos de pago incluyen datos de tarjeta reales de una tarjeta de pago, transmitir los datos de pago de la capa de seguridad de POS a una aplicación de seguridad de servidor instalada en un servidor de POS, proporcionar datos de pago falsos de la capa de seguridad de POS a una aplicación de terminal de POS instalada en el terminal de POS, donde los datos de pago falsos pueden procesarse como si fueran los datos de pago, de manera que el terminal de POS puede transmitir una primera solicitud de autorización al servidor de POS usando los datos de pago falsos, y transmitir una segunda solicitud de autorización del servidor de POS a un servidor remoto, donde la segunda solicitud de autorización puede incluir al menos los datos de pago.

Un método para asegurar transacciones de tarjeta de pago en un POS puede incluir interceptar datos de pago de un terminal de POS, donde los datos de pago pueden incluir datos de tarjeta reales de una tarjeta de pago, transmitir los datos de tarjeta reales del terminal de POS a una aplicación de seguridad de pasarela instalada en un servidor de pasarela, recibir, en el terminal de POS, datos de tarjeta falsos, los datos de tarjeta falsos configurados para procesarse en lugar de los datos de tarjeta reales, y proporcionar los datos de tarjeta falsos al terminal de POS, de manera que el terminal de POS puede transmitir una solicitud de autorización que incluye los datos de tarjeta falsos.

Un sistema de procesamiento de tarjeta de pago para asegurar transacciones de tarjeta de pago en un POS puede incluir un terminal de POS que puede incluir un ordenador anfitrión y un dispositivo de entrada de tarjeta, donde el ordenador anfitrión puede tener una aplicación de terminal de POS instalada en el mismo, un servidor de POS en comunicación con el terminal de POS a través de una red, donde el servidor de POS puede tener una aplicación de servidor de POS instalada en el mismo que comunica con la aplicación de terminal de POS para procesar transacciones de tarjeta de pago, una capa de seguridad de POS instalada en el ordenador anfitrión del terminal de POS, donde la capa de seguridad de POS puede al menos (a) interceptar datos de tarjeta reales recibidos del dispositivo de entrada de tarjeta cuando un usuario inicia una transacción de tarjeta de pago, (b) pasar datos de tarjeta falsos a la aplicación de terminal de POS para su uso en lugar de los datos de tarjeta reales, de manera que los datos de tarjeta falsos se transmiten al servidor de POS en lugar de los datos de tarjeta reales, y (c) transmitir los datos de tarjeta reales al servidor de POS, y una aplicación de seguridad de servidor instalada en el servidor de POS, donde la aplicación de seguridad de servidor puede estar en comunicación con la capa de seguridad de POS a través del canal seguro, donde la aplicación de seguridad de servidor puede recibir los datos de tarjeta reales de la capa de seguridad de POS a través del canal seguro y usar los datos de tarjeta falsos para procesar la transacción de tarjeta de pago.

Ni este resumen ni la siguiente descripción detallada pretenden definir la invención. La invención se define por las reivindicaciones 1-8.

Breve descripción de los dibujos

La Figura 1 es un diagrama de bloques ejemplar que ilustra un sistema de punto de venta de la técnica anterior;
La Figura 2 es un diagrama de bloques ejemplar que ilustra una realización de un sistema en punto de venta;
La Figura 3 es un diagrama de flujo de proceso ejemplar que ilustra una realización de un proceso de autorización de tarjeta de pago;
La Figura 4 es un diagrama de flujo de proceso ejemplar que ilustra otro ejemplo de un proceso de autorización de tarjeta de pago;
La Figura 5 es un diagrama de flujo ejemplar que ilustra un ejemplo de un proceso para invocar un componente de seguridad;
La Figura 6 es un diagrama de flujo ejemplar que ilustra otro ejemplo de un proceso para invocar un componente de seguridad;
La Figura 7 es un diagrama de flujo ejemplar que ilustra una realización de un proceso para encriptar datos de pago;
La Figura 8 es un diagrama de bloques ejemplar que ilustra ciertas realizaciones de datos de pago; y
La Figura 9 es un diagrama de flujo ejemplar que ilustra una realización de un proceso para realizar autorizaciones o liquidaciones incrementales.

Descripción detallada de realizaciones ejemplares

Las realizaciones específicas de la invención se describirán ahora con referencia a los dibujos. Estas realizaciones se pretenden para ilustrar, y no limitar, la presente invención.

La expresión "tarjeta de pago" abarca al menos tarjetas de crédito, tarjetas de débito, tarjetas bancarias, tarjetas inteligentes, tarjetas de cajero automático (ATM) y tarjeta de regalos. Además, otras formas de pago pueden intercambiarse con las tarjetas de pago descritas en el presente documento, que incluyen dispositivos activados para RFID, dispositivos inalámbricos, y otros dispositivos electrónicos o magnéticos que contienen datos de pago. Además, aunque la expresión tarjeta de pago se usa a través de todo el documento, ciertas realizaciones de los sistemas y métodos pueden usarse también para procesar tarjetas de identificación tal como permisos de conductor, tarjetas de acceso de seguridad, tarjetas de cobro de cheques y similares. Por ejemplo, en lugar de obtener la autorización de una tarjeta de pago, diversos ejemplos de los sistemas y métodos descritos en el presente documento pueden usarse para transmitir de manera segura y almacenar datos de tarjeta de identificación.

Para ilustrar adicionalmente los problemas de sistemas de pago actualmente disponibles, la Figura 1 representa un sistema de pago de la técnica anterior en un punto de venta. El punto de venta puede ser un punto de venta en un lugar de negocio del comerciante al que un cliente presenta una tarjeta de pago para compra o alquiler de bienes y servicios. El punto de venta también puede considerarse más en general como el lugar de negocio del comerciante. El punto de venta puede incluir, por ejemplo, una caja registradora, una interfaz de pago en una bomba de gas, un cajero de restaurante, una recepción en un hotel, un mostrador de alquiler de coches o similares. En algunas localizaciones, tal como hoteles, puede haber múltiples puntos de venta, tales como la recepción, en un restaurante y en una tienda de regalos. Independientemente de la localización del POS 20, a menudo no se transmiten datos de pago de manera segura de un punto a otro y/o se almacenan sin protección adecuada.

El sistema de pago incluye un terminal 20 de POS. El terminal 20 de POS incluye un dispositivo 2 de entrada de tarjeta y un ordenador 6 de anfitrión. El dispositivo 2 de entrada de tarjeta es un teclado de pin, lector de pasada de tarjeta, teclado informático o similares y se usa para capturar o introducir los datos de pago. El dispositivo 2 de entrada de tarjeta transmite los datos de pago al ordenador anfitrión 6 a través del enlace 4, que es un cable o similares. El ordenador anfitrión 6 puede ser una caja registradora, estación de trabajo, ordenador de sobremesa, o similares.

En muchos casos, el enlace 4 no es seguro puesto que no se usa encriptación en el enlace 4 para proteger los datos de pago. Sin embargo, incluso cuando se usa encriptación, el dispositivo 2 de entrada de tarjeta aún no será seguro entre el punto de recepción de los datos de pago y el punto de encriptación. Un registrador de teclas de software o hardware, por ejemplo, que residiera en el dispositivo 2 de entrada de tarjeta o incluso en el ordenador anfitrión 6 podría interceptar los datos de pago antes de la encriptación de esos datos. Por lo tanto, tanto el dispositivo 2 de entrada de tarjeta como el enlace 4 son vulnerables a robo de datos de pago.

El ordenador anfitrión 6 ejecuta una aplicación 10 de terminal de POS. La aplicación 10 de terminal de POS es responsable de recibir los datos de pago del dispositivo 2 de entrada de tarjeta. La aplicación 10 de terminal de POS envía los datos de pago junto con una solicitud de autorización, para determinar si la tarjeta de pago tiene suficientes fondos, a un servidor 8 de POS a través de una red 12. Como el dispositivo 2 de entrada de tarjeta, la aplicación 10 de terminal de POS en el ordenador anfitrión 6 puede estar comprendida por software maligno, software espía, registradores de teclas, virus, o similares. Además, la red 12 puede transferir datos de pago desencriptados al servidor 8 de POS, creando vulnerabilidades para empaquetar detectores de paquetes, que interceptan y registran tráfico de red.

El servidor 8 de POS es un ordenador típicamente localizado en el lugar de negocio del comerciante o en una localización remota de propiedad y operada por el comerciante. El servidor 8 de POS ejecuta una aplicación 14 de servidor de POS, que recibe los datos de pago y solicitud de autorización de la aplicación 10 de terminal de POS. La aplicación 14 de servidor de POS transmite los datos de pago para autorización a una pasarela 22, que solicita autorización de un procesador de tarjeta en comunicación con una entidad de autoridad.

La aplicación 14 de servidor de POS también almacena datos de transacción y datos de registro, ambos de los cuales incluyen los datos de pago, en una base de datos 16. Los datos de transacción se almacenan para posibilitar que el comerciante procese autorizaciones y liquidaciones incrementales, tales como autorizaciones de propina de restaurante y devoluciones de coche de alquiler (véase la Figura 9 para detalles adicionales). Los datos de registro se almacenan, entre otras razones, para que un técnico pueda resolver problemas del terminal 20 de POS. Una desventaja de almacenar datos de pago en el terminal 20 de POS es que numerosos números de tarjeta de pago se almacenan en forma desencriptada en una única localización, que proporciona acceso relativamente fácil para que un ladrón obtenga estos datos desprotegidos.

Volviendo a la Figura 2, se muestra un sistema de POS mejorado, que reduce o elimina al menos algunos de los problemas hallados en la técnica. Diversos componentes del sistema de POS protegen datos de pago en el dispositivo 28 de entrada de tarjeta y durante la transición de un terminal 30 de POS a un servidor 36 de POS. Además, diversos componentes del sistema de POS reducen la cantidad de datos de pago almacenados en el lugar de negocio del

comerciante. En consecuencia, ciertas realizaciones del sistema de POS superan algunos o todos los problemas anteriormente descritos.

El terminal 30 de POS es un sistema informático para recibir datos de pago y solicitar autorizaciones de tarjeta de pago. Por ejemplo, el terminal 30 de POS puede ser un terminal informático y dispositivo de pasada de tarjeta en una línea de caja de comestibles. El terminal 30 de POS de ciertas realizaciones incluye una combinación de componentes de software y de hardware.

Un negocio puede tener múltiples terminales 30 de POS, comunicando cada uno con un único servidor 36 de POS. Algunos hoteles, por ejemplo, incluyen terminales 30 de POS en la recepción, en el restaurante del hotel, y en la tienda de regalos del hotel, todos los cuales están conectados por una red a un servidor de POS común 36. En otro ejemplo, una tienda minorista o de comestibles puede incluir terminales 30 de POS en cada línea de caja.

El terminal 30 de POS y el servidor 36 de POS pueden ser idénticos al terminal de POS y al servidor del sistema de la técnica anterior de la Figura 1 pero ampliados con una capa de seguridad de POS (PSL) 40 y la aplicación de seguridad de servidor (SSA) 48. Estos dos componentes de software pueden añadirse a un sistema de pago preexistente que ya está desplegado para asegurar de manera efectiva el sistema.

Los terminales 30 de POS pueden realizar funciones especializadas en diferentes ajustes. Por ejemplo, un terminal 30 de POS de restaurante puede procesar una autorización inicial y una autorización incremental posterior para procesar una propina. Un terminal 30 de POS en un establecimiento de alquiler de coche u hotel puede pre-autorizar un coche o habitación para un cierto número de días, y a continuación solicitar más tarde autorización adicional cuando el coche se devuelve tarde o cuando un huésped se retira tarde de la habitación. Estas funciones especializadas se describen adicionalmente en relación con la Figura 9, a continuación.

En ciertas realizaciones, el terminal 30 de POS incluye un dispositivo 28 de entrada de tarjeta y un ordenador 34 de anfitrión. El dispositivo 28 de entrada de tarjeta es un teclado de pin, lector de pasada de tarjeta, teclado informático, pantalla táctil, o similar. Algunas implementaciones del terminal 30 de POS no incluyen el dispositivo 28 de entrada de tarjeta, sino en su lugar un componente de software que actúa como un dispositivo de entrada de tarjeta. Por ejemplo, una pantalla de pago en un escaparate de Internet puede actuar como un dispositivo de entrada de tarjeta.

El dispositivo 28 de entrada de tarjeta de diversas realizaciones recibe datos de pago de cualquier medio de pago. El medio de pago puede ser una tarjeta de pago, chip electrónico, dispositivo de identificación por frecuencia de radio (RFID), o similares. Los datos de pago pueden ser datos codificados en una banda magnética en la parte trasera de una tarjeta, datos almacenados en un chip electrónico, datos almacenados en un dispositivo de RFID, o cualquier otra forma de datos almacenados. Como se analiza a continuación con respecto a la Figura 8, los datos de pago pueden incluir rastrear datos almacenados en la parte trasera de una tarjeta de pago.

Los datos de pago pueden incluir también un número de cuenta personal (PAN), número de identificación personal (PIN), fecha de caducidad, nombre de titular y/o un código de seguridad de tarjeta, por ejemplo, un código de tres dígitos comúnmente hallado en la parte trasera de las tarjetas de pago. Además, los datos de pago pueden incluir una firma de titular electrónica o datos biométricos, tal como una huella dactilar digital. Los datos de pago pueden incluir también un código de seguridad dinámico, tal como puede hallarse en un dispositivo de identificación por frecuencia de radio (RFID) embebido en una tarjeta de pago. Pueden proporcionarse también muchas otras formas de datos de pago.

El dispositivo 28 de entrada de tarjeta pasa los datos de pago al ordenador 34 anfitrión. En un ejemplo, el dispositivo 28 de entrada de tarjeta está conectado al ordenador 34 anfitrión a través de un enlace 32. El enlace 32 es típicamente un cable, serie (por ejemplo, RS232 o USB), paralelo, Ethernet, u otra interfaz de hardware. Como alternativa, no se proporciona el enlace 32 y el dispositivo 28 de entrada de tarjeta es integral con el ordenador 34 anfitrión. En otro ejemplo, el enlace 32 es una interfaz de software, tal como un zócalo de red, o alguna combinación de hardware y software.

El ordenador 34 anfitrión puede implementarse como una caja registradora o puede estar conectado con una caja registradora. Típicamente, el ordenador 34 anfitrión es o comprende un ordenador de fin general (por ejemplo, un PC). El ordenador 34 anfitrión recibe datos de pago del dispositivo 28 de entrada de tarjeta, procesa los datos, y transmite solicitudes de autorización al servidor 36 de POS. Cuando el servidor 36 de POS transmite respuestas de autorización al ordenador 34 anfitrión, el ordenador 34 anfitrión visualiza la respuesta al titular y procesa una transacción de pago.

El ordenador 34 anfitrión en un ejemplo ejecuta un sistema operativo (no mostrado), tal como Windows, Linux, Unix, o similares. El ordenador 34 anfitrión también incluye la aplicación 38 de terminal de POS y la capa de seguridad de POS (PSL) 40. En ciertos ejemplos, la aplicación 38 de terminal de POS y la PSL 40 son componentes de software, que pueden implementarse como guiones, programas ejecutables, código de bytes interpretado, o similares.

En una implementación, la PSL 40 es una aplicación de bajo nivel con relación a la aplicación 38 de terminal de POS. Por ejemplo, la PSL 40 preferentemente tiene prioridad a través de la aplicación 38 de terminal de POS para acceder

a rutinas y datos de sistema operativo. Además, la PSL 40 preferentemente puede interceptar datos pretendidos para transmisión a la aplicación 38 de terminal de POS, tal como datos de pago. La PSL 40 puede ejecutarse como un proceso de sistema operativo.

La PSL 40 en una implementación es un guion que se ejecuta en un nivel suficientemente bajo en el ordenador 34 anfitrión para capturar los datos de pago antes de que la aplicación 38 de terminal de POS reciba los datos de pago. En un ejemplo, la PSL 40 captura los datos de pago monitorizando y/o accediendo a una memoria intermedia de entrada en el dispositivo 28 de entrada de tarjeta o en el ordenador 34 anfitrión. La PSL 40 puede también estar a un nivel suficientemente bajo para evitar programas maliciosos, tales como registradores de teclas, detectores de paquetes, software espía y virus que obtienen los datos de pago. Además, la PSL 40 encripta los datos de pago y transmite los datos de pago encriptados al servidor 36 de POS.

El terminal 30 de POS comunica con el servidor 36 de POS a través de una red 42. La red 42 puede incluir cables, encaminadores, conmutadores, y otro hardware de red. Además, la red 42 puede ser una red inalámbrica, que tiene encaminadores inalámbricos, puntos de acceso, y similares. En un ejemplo, la red 42 es la misma o similar a la red 12 usada en el sistema de la técnica anterior de la Figura 1. Sin embargo, además de la red 12, la red 42 se hace segura mediante la adición de un canal 44 seguro. En una implementación, la aplicación 38 de terminal de POS y la aplicación 46 de servidor de POS se comunican a través de un canal no seguro en la red 42, y la PSL 40 y una aplicación de seguridad de servidor (SSA) 48 que reside en el servidor 36 de POS comunica a través del canal 44 seguro. El canal 44 es seguro en diversas implementaciones puesto que los datos encriptados se transmiten entre la PSL 40 y la SSA 48 a través del canal 44.

El servidor 36 de POS es un sistema informático que recibe solicitudes de autorización de uno o más terminales 30 de POS y transmite la solicitud de autorización a un servidor remoto, por ejemplo, una pasarela 52 a través de la Internet 18, una red de área extensa (WAN), una red de área local (LAN), o una línea alquilada. El servidor 36 de POS por lo tanto actúa como una interfaz entre el terminal o terminales 30 de POS y la pasarela 52. El servidor 36 de POS puede estar localizado en un lugar de negocio del comerciante. Como alternativa, el servidor 36 de POS está localizado en un centro de datos remoto, que puede ser de propiedad o estar alquilado por el comerciante.

Además de realizar autorizaciones, el servidor 36 de POS de ciertos ejemplos también realiza liquidaciones. Al cierre del negocio o a la siguiente mañana antes de la apertura, el comerciante, usando el servidor 36 de POS, envía todas sus transacciones autorizadas al servidor remoto (por ejemplo, la pasarela 52). Este grupo de transacciones se denomina típicamente como una liquidación de lote. Emitiendo una liquidación el servidor 36 de POS posibilita que el comerciante reciba pago o un crédito para pago en las transacciones de tarjeta de crédito autorizada del día, que incluye transacciones con tarjetas de débito usadas como tarjetas de crédito. En algunos ejemplos, donde se procesan las tarjetas de débito como débito, el comerciante recibe pago del banco sin usar una liquidación de lote. Cuando las tarjetas de pago son tarjetas de regalo, tampoco se usa a menudo la liquidación.

Como se muestra en la realización representada de la Figura 2, el servidor 36 de POS incluye una aplicación 46 de servidor de POS y la SSA 48. En ciertos ejemplos, la aplicación 46 de servidor de POS y la SSA 48 son componentes de software, que pueden implementarse como guiones, programas ejecutables, código de bytes interpretado o similares.

En una implementación, la aplicación 46 de servidor de POS es una aplicación de alto nivel con relación a la SSA 48. Por ejemplo, la SSA 48 puede tener prioridad sobre la aplicación 46 de terminal de POS para acceder a las rutinas y datos de sistema operativo. En otro ejemplo, la SSA 48 puede interceptar datos pretendidos para su transmisión a la aplicación 46 de servidor de POS. En otros ejemplos más, la SSA 48 ejecuta un proceso de sistema operativo. Como alternativa, la SSA 48 no es una aplicación de nivel inferior que la aplicación 46 de servidor de POS.

La SSA 48 de ciertos ejemplos sustituye un componente de comunicaciones preexistente o es una modificación del mismo. Como un componente de comunicaciones, la SSA 48 en una implementación envía y recibe solicitudes de autorización y liquidaciones a un servidor remoto, tal como una pasarela. Puesto que la SSA 48 actúa como el componente de comunicaciones preexistente, la aplicación 46 de servidor de POS puede comunicar con la SSA 48 como si la SSA 48 fuera el componente de comunicaciones preexistente. La SSA 48 de ciertos ejemplos posibilita por lo tanto ventajosamente que la aplicación 46 de servidor de POS envíe datos de pago falsos a la SSA 48 sin modificación alguna a la aplicación 46 de servidor de POS.

La SSA 48 y la PSL 40 pueden monitorizarse entre sí para validar versiones de producto y para asegurar que el sistema no se ha manipulado. Esta disposición de monitorización inhibe que un robo o código malicioso altere la SSA 48 o PSL 40 para desviar, por ejemplo, datos de pago a terceros.

En una realización, la PSL 40 encripta los datos de pago interceptados y envía los datos de pago encriptados a la SSA 48 a través del canal 44 seguro. La SSA 48 desencripta los datos de pago encriptados y crea datos de pago falsos sustituyendo toda o una porción de los datos de pago con datos falsos. La SSA 48 re-encripta los datos de pago y almacena los datos de pago encriptados en el servidor 36 de POS. Posteriormente, la SSA 48 transmite los datos de pago falsos a la PSL 40 a través del canal 44 seguro. La PSL 40 a continuación proporciona los datos de pago falsos

a la aplicación 38 de terminal de POS en lugar de los datos de pago reales. La aplicación 38 de terminal de POS procesa los datos de pago falsos como si fueran datos de pago reales, proporcionando los datos de pago falsos a la aplicación 46 de servidor de POS a través del canal 42 no seguro como parte de una solicitud de autorización. Como alternativa, la aplicación 38 de terminal de POS proporciona los datos de pago falsos a la aplicación 46 de servidor de POS a través del canal 44 seguro. Sin embargo, incluso cuando la aplicación 38 de terminal de POS envía los datos de pago falsos a través del canal 42 no seguro, el sistema aún está seguro ya que los datos de pago no reales se almacenan en una base de datos 50.

En realizaciones alternativas, la PSL 40, en lugar de la SSA 48, crea los datos de pago falsos. La PSL 40 en tales realizaciones a continuación envía los datos de pago falsos a través del canal 44 seguro a la SSA 48.

La aplicación 48 de servidor de POS también procesa los datos de pago falsos como si fueran datos de pago reales. En consecuencia, la aplicación 48 de servidor de POS almacena los datos de pago falsos en la base de datos 50 en lugar de los datos de pago reales. Análogamente, los datos de registro comúnmente mantenidos por la aplicación 46 de servidor de POS también incluyen datos de pago falsos en lugar de datos de pago reales. Por lo tanto, en ciertos ejemplos, no se almacenan datos de pago reales en el punto de venta (o se almacenan únicamente de manera temporal en ciertos puntos en el proceso de autorización y se borran posteriormente). Incluso si los datos de pago falsos incluyen una porción de los datos de pago reales (véase la Figura 8), no se almacenan datos de pago reales completos en el punto de venta.

La aplicación 46 de servidor de POS transmite los datos de pago falsos a la SSA 48. La SSA 48 en una realización a continuación combina los datos de pago falsos con los datos de pago encriptados y transmite los datos de pago falsos y de pago reales combinados a través de la Internet 18, línea alquilada, u otra red al servidor remoto (por ejemplo, la pasarela 52) como parte de una solicitud de autorización. La SSA 48 en otra realización envía únicamente los datos de pago reales o únicamente los datos de pago falsos a la pasarela 52. Además, la SSA 48 puede enviar los datos de pago reales y los datos de pago falsos a la pasarela 52 en transmisiones separadas. En una realización, la SSA 48 por lo tanto borra todos los datos de pago re-encriptados. Como alternativa, la SSA 48 espera una respuesta de la pasarela 52 antes de borrar los datos de pago re-encriptados.

La pasarela 52 en un ejemplo incluye uno o más sistemas informáticos que actúan como servidores (o que actúan de manera colectiva como un servidor), remotos del servidor 36 de POS. En diversas realizaciones, la pasarela 52 se mantiene por un proveedor de servicio de aplicación (ASP), que proporciona servicios de aplicación y almacenamiento de datos para comerciantes. La pasarela 52 puede mantenerse también por un procesador de tarjeta, asociación de tarjeta, banco emisor, u otra entidad. Por ejemplo, la pasarela 52 puede usarse como un servidor de procesador de tarjeta, de manera que el servidor 36 de POS comunica directamente (o a través de uno o más intermediarios) con el procesador de tarjeta. En algunas implementaciones, la pasarela 52 comunica con el servidor 36 de POS a través de una línea alquilada o red de área extensa (WAN), y de esta manera actúa como una zona desmilitarizada (DMZ) entre la red de comerciante, que incluye los terminales 30 de POS y el servidor 36 de POS, y fuera del mundo. La pasarela 52 en estas implementaciones añade por lo tanto una capa adicional de seguridad de ataques exteriores. La pasarela 52 puede comunicar también con una entidad de autoridad usando una línea alquilada.

Una capa de seguridad de pasarela (GSL) 56 que reside en la pasarela 54 separa los datos de pago falsos y datos recibidos de pago re-encriptados combinados del servidor 36 de POS. La capa 56 de seguridad de pasarela desencripta los datos de pago re-encriptados y pasa los datos de pago a una aplicación 54 de pasarela, que en un ejemplo (por ejemplo, cuando la pasarela 52 no se mantiene por un procesador de tarjeta) transmite los datos de pago a un procesador de tarjeta para autorización. Como alternativa, la aplicación 54 de pasarela transmite los datos de pago re-encriptados, o en otro ejemplo, encripta los datos de pago con un esquema de encriptación diferente. Tras recibir una respuesta a la solicitud de autorización, la GSL 56 transmite la respuesta de autorización junto con los datos de pago falsos al servidor 36 de POS. Proporcionando los datos de pago falsos al servidor 36 de POS, la GSL 56 posibilita que el servidor 36 de POS identifique la respuesta de autorización con la tarjeta de pago correcta (como se representa como los datos falsos), sin proporcionar los datos de pago reales.

Puesto que los datos de pago falsos se identifican con una tarjeta de pago específica, los datos de pago falsos pueden usarse como un testigo para una transacción adicional con la misma tarjeta de pago, tal como una autorización o liquidación incremental, como se describe en detalle adicional a continuación con respecto a la Figura 9. Cuando se solicita una transacción adicional que usa una tarjeta de pago por el servidor 36 de POS, el servidor 36 de POS puede enviar el testigo que corresponde a esa tarjeta de pago a la pasarela 52 para realizar la transacción adicional. La pasarela 52 hace coincidir el testigo con los datos de pago reales almacenados en la pasarela 52 para solicitar autorización o liquidación de una entidad de autoridad. En lugar de devolver los datos de pago falsos como un testigo, sin embargo, la GSL 56 de algunos ejemplos puede devolver también un conjunto diferente de datos falsos como un testigo. Estos datos falsos en algunos casos pueden ser una porción o derivada de los datos de pago falsos.

La pasarela 52 también facilita la realización de liquidaciones de lote en ciertos ejemplos. En un ejemplo, el terminal 30 de POS envía información de transacción de fin del día a la SSA 36, que solicita la liquidación. La SSA 36 transmite los datos falsos que corresponden a la información de transacción de fin del día a la pasarela 52. La pasarela 52 usa componentes de los datos falsos para actualizar cantidades de transacción finales para que se liquiden.

Por lo tanto, puede observarse que en diversos puntos de vulnerabilidad en el sistema de POS de la Figura 1, se aseguran los datos de pago. Por ejemplo, la PSL 40 evita que se envíen datos de POS en forma evidente a la aplicación 38 de terminal de POS. Además, la PSL 40 transmite una versión encriptada de los datos a través de un canal 44 seguro a la SSA 48. La SSA 48 asegura datos de transacción y registra datos almacenados en la base de datos 50 usando datos falsos y por lo tanto no se almacenan datos de titular o muy pocos en la base de datos 50. Además, la GSL 46 asegura transacciones almacenando datos de pago reales en una localización segura y transmitiendo datos de pago falsos o datos de testigo de vuelta al servidor 36 de POS. En consecuencia, las oportunidades para obtener de manera inapropiada datos de pago se reducen o eliminan de manera completa.

La Figura 3 ilustra el proceso de autorización de tarjeta anteriormente descrito de acuerdo con una realización. En la etapa 1, la PSL 40 se invoca directamente por una acción de usuario, indirectamente en respuesta a la entrada de datos de pago, o por programación, por ejemplo, por otro programa tal como la aplicación 38 de terminal de POS. En un ejemplo donde la PSL se invoca directamente por acción de usuario, se usa una tecla de acceso rápido para invocar la PSL. La tecla de acceso rápido puede estar localizada en el terminal de POS 24 o en un dispositivo de entrada de tarjeta tal como el dispositivo 28 de entrada de tarjeta de la Figura 2. La tecla de acceso rápido puede ser una tecla en un teclado, teclado de pin, pantalla informática, o pantalla táctil. En un ejemplo, la tecla de acceso rápido es una tecla de "débito" o "crédito" en un teclado de pin, presentada por el titular. En otra realización, la tecla de acceso rápido es una tecla de tarjeta de pago presionada por un empleado del comerciante.

Adicionalmente, la acción de usuario puede incluir el uso de una tarjeta de entrada manual, que es una tarjeta usada por un empleado del comerciante y está configurada para posibilitar que el cliente introduzca manualmente datos de pago a través de un teclado de pin, teclado o similares. El uso de una tarjeta de clave manual se describe en mayor detalle a continuación en relación con las Figuras 5-6.

En ejemplos donde se invoca la PSL 40 indirectamente por un evento de entrada de datos de pago, el evento de entrada de datos de pago puede incluir una pasada de tarjeta o entrada manual de datos de pago realizada por un titular (por ejemplo, un cliente) o por un empleado del comerciante. En un ejemplo donde la PSL 40 se invoca por programación, el terminal de POS puede hacer una llamada de función usando, por ejemplo, una biblioteca dinámica enlazada (DLL), que invoca una PSL 40.

En la etapa 2, la PSL 40 visualiza una interfaz de usuario de pago (pantalla de visualización) en la pantalla del dispositivo 28 de entrada de tarjeta. La interfaz de usuario de pago en un ejemplo se visualiza en lugar de una interfaz de usuario de pago preexistente asociada con la aplicación 46 de servidor de POS. La interfaz de usuario de pago en una realización es una pantalla de pago sustituta, que posibilita que un usuario (por ejemplo, titular o empleado del comerciante) proporcione datos de pago directamente a la PSL 40. La pantalla de pago sustituta puede proporcionar también tranquilidad para el usuario visualizando un mensaje que describe que los datos de pago son seguros. En un ejemplo alternativo, la pantalla de pago sustituto se oculta del usuario y por lo tanto es transparente para el usuario.

La interfaz de usuario de pago de algunas realizaciones emerge sobre o se superpone de otra manera o sustituye la interfaz de usuario prexistente. La interfaz de usuario de pago puede tener una apariencia y aspecto similar a la interfaz de usuario preexistente, o la interfaz de usuario de pago puede tener una apariencia y aspecto diferente. En otros ejemplos, la interfaz de usuario de pago es la interfaz de usuario prexistente en lugar de una interfaz de usuario de pago sustituta.

La PSL 40 también captura datos de pago proporcionados por el titular. La PSL 40 de ciertos ejemplos intercepta los datos de pago y evita que otros programas accedan a los datos. Capturando los datos de pago antes de otros programas que capturan los datos, la PSL 40 en diversas implementaciones actúa como un registrador de teclas.

En una realización, la PSL 40 es un registrador de teclas basado en gancho, por ejemplo, un registrador de teclas que usa rutinas de sistema operativo (por ejemplo, la API (Interfaz de Programación de Aplicación) SetWindowsHookEx en implementaciones de Windows) para capturar de datos de entrada. De manera similar, la PSL 40 puede usar otras rutinas de sistema operativo (por ejemplo, la API GetKeyboardState en implementaciones de Windows) para obtener pulsaciones de tecla antes de que las pulsaciones de tecla se reciban por cualquier ventana activa. Como alternativa, la PSL 40 puede ser un registrador de teclas basado en núcleo, que recibe solicitudes de entrada/salida (E/S) que se envían al controlador del dispositivo de entrada (por ejemplo, el dispositivo 28 de entrada de tarjeta). En un ejemplo de este tipo, la PSL 40 emplea un controlador de nivel de dispositivo que se sitúa por encima del controlador de teclado (por ejemplo, entre el controlador de dispositivo de entrada y otras funciones o aplicaciones de sistema operativo), y por lo tanto puede interceptar solicitudes de E/S. Además, la PSL 40 puede ser también un registrador de teclas de inyección de manejador que inyecta caracteres en una ventana y desviando por lo tanto el dispositivo de entrada. Como un registrador de teclas, la PSL 40 captura pulsaciones de tecla del teclado de pin, pulsaciones de teclas de teclado, rastrea datos, datos de firma, datos biométricos, y similares. Capturar estos datos permite que la PSL 40 evite que programas maliciosos accedan a los datos y también permite que la PSL 40 evite que los datos alcancen la aplicación 38 de terminal de POS. Por lo tanto, la PSL 40 de ciertos ejemplos aumenta la seguridad del terminal 30 de POS.

Volviendo a la etapa 3, la PSL 40 transmite los datos de pago capturados a la SSA 48 a través de un canal seguro. En una realización, el canal es seguro debido a un esquema de encriptación realizado por la PSL 40 en los datos de pago. El esquema de encriptación puede incluir una clave pública/privada mixta (clave asimétrica/simétrica), una clave pública, una clave privada, u otro esquema de encriptación. En una realización, se usa un protocolo IPSEC o PKI en el esquema de encriptación. Una implementación de ejemplo del esquema de encriptación incluye una clave pública/privada mixta almacenada en tiempo real, en memoria de acceso aleatorio (RAM). La encriptación y desencriptación puede ser dinámica en su naturaleza, en que el esquema de encriptación puede crear una nueva clave pública/privada cada vez que se inicia la SSA 48. Además, las claves en el esquema de encriptación pueden implementarse usando uno o más algoritmos de encriptación. Por ejemplo, puede usarse un algoritmo blowfish, algoritmo twofish, un algoritmo de 3DES (Norma de Encriptación de Datos Triple) o AES (Norma de Encriptación Avanzada) u otro algoritmo para encriptar los datos de pago en la PSL 40.

La SSA 48 en una realización desencripta los datos de pago encriptados y devuelve datos de pago falsos a la PSL 40 en la etapa 4. Como alternativa, la SSA 48 no encripta los datos de pago. La SSA 48 genera datos de pago falsos de manera que el terminal 30 de POS y el servidor 36 de POS podrán procesar los datos de pago falsos como si fueran datos de pago reales. En una realización, la SSA 48 genera los datos de pago falsos usando un generador de números aleatorios. En otra realización, la SSA 48 genera los datos de pago falsos de manera secuencial. Por ejemplo, un número de cuenta personal (PAN) de una primera tarjeta de pago puede sustituirse por números de una secuencia de datos falsos, y una segunda PAN puede sustituirse por números sucesivos en la secuencia de datos falsos. Se describe a continuación un ejemplo más detallado de datos falsos con respecto a la Figura 8.

La SSA 48 re-encripta los datos de pago o proporciona encriptación adicional a datos de pago ya encriptados. La SSA 48 almacena los datos de pago encriptados en el servidor 36 de POS. En algunas implementaciones, la SSA 48 proporciona encriptación adicional incluso cuando los datos de pago ya están encriptados puesto que la SSA 48 puede usarse sin la PSL 40 para procesar transacciones del servidor 36 de POS y/o terminal de POS 30. En tales circunstancias, puede ser deseable encriptar cualesquiera datos transmitidos de la SSA 48 a través de una red pública. Adicionalmente, puede encriptarse otra información no pública que ya puede existir en el servidor 36 de POS y enviarse a un centro de datos usando la SSA 48. Dependiendo del comerciante, esta información puede incluir información pre-registrada tal como números de Seguridad Social, ID de pacientes médicos, direcciones, y similares.

En un ejemplo, la SSA 48 proporciona dos tipos de datos de pago encriptados, que incluyen una versión "que no puede desencriptarse" y una versión que puede desencriptarse. La versión que no puede desencriptarse puede desencriptarse en la pasarela 52 pero no en la localización del comerciante (por ejemplo, en el terminal 30 de POS o servidor 36 de POS), y la versión que puede desencriptarse puede desencriptarse en la localización del comerciante. Como se describe más completamente a continuación en relación con la Figura 7, la versión que no puede desencriptarse puede usarse para procesar transacciones de crédito y las transacciones de débito fuera de línea, y la versión que puede desencriptarse puede usarse para procesar transacciones de débito en línea. Sin embargo, en ejemplos alternativos, tal como cuando no se usan transacciones de débito en línea por el comerciante, la SSA 48 proporciona únicamente una versión que no puede desencriptarse de los datos de pago. Además, en aún otras realizaciones, la PSL 40, en lugar de la SSA 48, proporciona las versiones que no pueden desencriptarse y que pueden desencriptarse de datos de pago encriptados cuando la PSL 40 encripta originalmente los datos de pago. En un ejemplo de este tipo, la SSA 48 proporciona encriptación adicional a los datos de pago ya encriptados. Además, la SSA 48 puede generar datos de pago falsos sin conocer los contenidos de los datos de pago reales.

En la etapa 5, la PSL 40 pasa los datos de pago falsos a la aplicación 38 de terminal de POS. La aplicación 38 de terminal de POS recibe los datos de pago falsos como si fueran los datos de pago reales. Puesto que la aplicación 38 de terminal de POS tiene únicamente datos de pago falsos, el software y hardware malicioso en comunicación con el terminal 30 de POS no pueden acceder a los datos de pago reales.

En la etapa 6, la aplicación 38 de terminal de POS pasa los datos de pago falsos a la aplicación 46 de servidor de POS en el servidor 36 de POS típicamente a través de un canal no seguro como parte de una solicitud de autorización. Puesto que se usan los datos falsos, los datos de pago se hacen seguros.

En la etapa 7, la aplicación 46 de servidor de POS registra la transacción con los datos de pago falsos en la base de datos 50. Los datos de transacción pueden incluir los datos de pago falsos junto con información con respecto un precio de compra, elementos comprados, y similares. Los datos de transacción se usan en algunas aplicaciones para generar informes, generando liquidaciones de lotes, y para procesar incrementos o autorizaciones (véase la Figura 9 a continuación). Además, la aplicación 46 de servidor de POS almacena datos de registro en la base de datos 50. Los datos de registro pueden incluir un subconjunto o todos de los datos de transacción y pueden incluir también datos adicionales. Los datos de registro pueden usarse para proporcionar acceso para que un técnico resuelva problemas del terminal 34 de POS o el servidor 36 de POS. Puesto que los datos de transacción y registro falsos se almacenan en la base de datos 50, los datos de pago son seguros.

En la etapa 8, la aplicación 48 de servidor de POS envía un mensaje de solicitud de pago o autorización a la SSA 46. Posteriormente, en la etapa 9 la SSA 46 modifica el mensaje de solicitud de pago combinando los datos de pago falsos con los datos de pago re-encriptados. La SSA 48 a continuación envía los datos de pago combinados a la capa de

seguridad de pasarela (GSL) 56 en la etapa 10.

En la pasarela 52, la GSL 56 a continuación desencripta los datos de pago encriptados en la etapa 11 para recuperar los datos de pago reales. La GSL 56 en la etapa 12 a continuación pasa los datos de pago reales a la aplicación 54 de pasarela. Como alternativa, la GSL 56 re-encripta los datos antes de enviar los datos a la aplicación 54 de pasarela. En otra realización, la GSL 56 no desencripta los datos encriptados recibidos del servidor 36 de POS, sino que en su lugar pasa los datos encriptados a la aplicación 54 de pasarela. En la etapa 13, la aplicación 54 de pasarela a continuación transmite los datos de pago a un procesador de tarjeta, que es un intermediario al obtener eventualmente una respuesta de autorización de una localización central tal como un banco emisor.

El procesador devuelve los datos de pago y una respuesta de solicitud de pago a la aplicación 54 de pasarela en la etapa 14. La aplicación 54 de pasarela pasa los datos de pago y la respuesta de solicitud de pago a la GSL 56 en la etapa 15. Posteriormente, la GSL 56 envía los datos de pago falsos, en lugar de los datos de pago reales, junto con la respuesta de solicitud de pago a la SSA 48. Enviando los datos falsos, la GSL 56 posibilita que la SSA 48 identifique la respuesta de solicitud de pago con la tarjeta de pago correcta sin enviar los datos de pago reales a la SSA 48.

Volviendo a la Figura 4, se representa un flujo de proceso alternativo para procesar transacciones de tarjeta de pago. Este flujo de proceso alternativo puede usarse, por ejemplo, con terminales 30 de POS heredados que tienen una interfaz de comunicaciones directa (por ejemplo, no mediante una SSA o similares) a una pasarela particular o plataforma de procesamiento (por ejemplo un extremo frontal del propietario del banco). En el flujo de proceso alternativo de la Figura 4, un terminal 30 de POS está en comunicación con una pasarela 64 y un servidor 8 de POS. Además, una base de datos 50 está en comunicación con, o se mantiene en, el servidor 8 de POS. En la etapa 1, la PSL 60 se invoca directamente por una acción de usuario, indirectamente en respuesta a la entrada de datos de pago, o por programación, por ejemplo, de una manera similar como se describe con respecto a la Figura 3 anterior.

Posteriormente, en la etapa 2 la PSL 60 visualiza una interfaz de usuario de pago y captura la información de pago. En la etapa 3, la PSL 60 envía la información de pago capturada a una aplicación 62 de seguridad de pasarela a través de un canal seguro, que puede ser la Internet, una línea alquilada, u otra red. En un ejemplo, la PSL encripta los datos antes de la transmisión, asegurando de esta manera el canal.

En la etapa 4, la GSA 66 devuelve datos de pago falsos a la PSL 60. En consecuencia, no se almacenan datos de pago reales en el terminal 34 de POS o el servidor 8 de POS. Sin embargo, si se usa una transacción de débito en línea, la GSA 66 puede proporcionar también una versión que puede desencriptarse de los datos de pago para posibilitar que el terminal 30 de POS procese la transacción de débito en línea. Como alternativa, la PSL 60 usa una versión que puede desencriptarse de los datos de pago para procesar la transacción de débito en línea. La PSL 60 en la etapa 5 pasa los datos de pago falsos a la aplicación 38 de terminal de POS. La aplicación 38 de terminación de POS procesa los datos de pago falsos como si fueran datos de pago reales.

La aplicación 38 de terminal de POS a continuación en la etapa 6 pasa los datos de pago falsos a la aplicación 14 de servidor de POS. En la etapa 7, la aplicación 14 de servidor de POS registra la transacción con los datos de pago falsos en la base de datos 50. Puesto que los datos de pago falsos se almacenan en la base de datos 50, los datos de pago son menos vulnerables a robo.

Posteriormente, la aplicación 14 de servidor de POS en la etapa 8 envía un mensaje de solicitud de pago o de solicitud de autorización a la pasarela 64 usando los datos de pago falsos. La aplicación 66 de seguridad de pasarela en la etapa 9 transmite los datos de pago reales y un mensaje de solicitud de pago a un procesador. Por lo tanto, excepto cuando los datos de pago reales encriptados se transmiten a la GSA 66, únicamente se usan datos de pago en la transacción de autorización. Finalmente, la pasarela recibe los datos de pago y la respuesta de solicitud de pago del procesador y reenvía la respuesta a la aplicación 46 de servidor de POS.

Ciertos componentes descritos en el flujo de proceso alternativo pueden proporcionarse a un sistema de POS no seguro preexistente para asegurar el sistema de POS. En un ejemplo, se proporciona la PSL 40 para mejorar o retroalimentar un sistema de POS existente. Además, puede proporcionarse la GSA 66 para sustituir o mejorar una pasarela 64 preexistente. Sin embargo, en la realización representada, no se añade componente para mejorar el servidor 8 de POS preexistente. Ventajosamente, se usan por lo tanto menos componentes para asegurar el sistema de POS en el flujo de proceso alternativo de la Figura 4.

Las Figuras 5 y 6 ilustran diversos ejemplos para invocar una PSL y capturar datos de pago. La Figura 5 representa un método 100 para invocar directamente una PSL y capturar datos de pago. La Figura 6 representa un método 200 para invocar indirectamente una PSL y capturar datos de pago. Los métodos 100, 200 pueden realizarse por cualquiera de los terminales de POS anteriormente descritos, y como parte del proceso de la Figura 3 o la Figura 4.

Haciendo referencia a la Figura 5, en 102, el método 100 determina si se ha detectado una acción de usuario. La acción de usuario puede incluir, por ejemplo, una presión de tecla de acceso rápido o una pasada de tarjeta de clave manual. Si no se ha detectado una acción de usuario, el método 100 vuelve a 102. En un ejemplo, el método en 102 por lo tanto escucha la presión de una tecla de acceso rápido, que puede ser una tecla en un teclado, teclado de pin,

un botón en un ordenador o pantalla táctil, o similares. La presión de una tecla de acceso rápido puede ser, por ejemplo, la presión de una tecla de "tipo de pago" en un teclado de pin del dispositivo de entrada de tarjeta.

Si se detecta una acción de usuario, el método 100 invoca la PSL en 104. En una realización, la PSL es residente en memoria antes de la presión de tecla, que escucha una acción de usuario, entrada de datos de pago, o llamada de programa (descrito a continuación con respecto a la Figura 6). En una realización de este tipo, se invoca la PSL activando funciones en la PSL que posibilitan la captura de datos de pago. En un ejemplo alternativo, se invoca la PSL que se carga en memoria.

En 106, el método 100 visualiza una pantalla de pago sustituta. En un ejemplo, la pantalla de pago es una pantalla de pago sustituta visualizada en lugar de una pantalla de pago original suministrada por un fabricante de POS. La pantalla de pago sustituta puede tener una apariencia y aspecto similar a la pantalla de pago original; sin embargo, los datos de pago introducidos en la pantalla de pago sustituta se capturan por la PSL. La pantalla de pago sustituta puede también parecer diferente de la pantalla de pago original o incluir menos o más características que la pantalla de pago original. La pantalla de pago sustituta posibilita la entrada de datos de pago directamente en la PSL.

El método 100 continúa en 108 determinando si la acción de usuario incluye la entrada de una tarjeta de clave manual. La tarjeta de clave manual en una implementación es una tarjeta usada por un empleado del comerciante para preparar el terminal de POS para recibir datos de entrada manual. Los datos de entrada manual incluyen datos de pago escritos en un teclado, teclado de pin, o similares, que pueden introducirse si el lector de pasada de tarjeta no está funcionando o no está disponible para el titular, tal como en transacciones en línea o de catálogo de teléfono. Si la acción de usuario incluye el uso de una tarjeta de clave manual, el método 100 continúa para capturar los datos introducidos manualmente en 110. De otra manera, si se usara otra acción de usuario, el método 100 continúa para capturar datos pasados de la tarjeta de pago en 112.

En otro ejemplo, la entrada manual de datos de pago puede hacerse sin usar una tarjeta de entrada manual. Por ejemplo, en un ejemplo, un titular invoca la PSL a través de una presión de tecla de acceso rápido e introduce los datos de pago en la pantalla de pago sustituta.

Haciendo referencia a la Figura 6, el método 200 determina si la entrada de datos de pago se ha detectado en 202. Si no se ha detectado la entrada de datos de pago, el método 200 vuelve a 202. En un ejemplo, el método en 202 por lo tanto escucha la entrada de datos de pago, que pueden incluir una pasada de tarjeta, entrada manual de datos de pago, o similares. La entrada de datos de pago puede realizarse por un titular o empleado del comerciante en diversas realizaciones.

Si se detectó la entrada de datos de pago, el método 200 invoca la PSL en 204, que captura los datos de pago en 206. En un ejemplo, la PSL es residente en memoria antes de la entrada de datos de pago, que escucha una acción de usuario (véase la Figura 5) o la entrada de datos de pago. En un ejemplo de este tipo, "invocar" la PSL significa activar la PSL para posibilitar que la PSL capture los datos de pago. En un ejemplo alternativo, la entrada de datos de pago invoca la PSL provocando que la PSL se cargue en memoria.

En un ejemplo, no se usa una pantalla de pago sustituta para capturar los datos de pago puesto que la entrada de datos de pago proporciona los datos de pago. En un ejemplo alternativo, la pantalla de pago sustituta también se visualiza en el método 200. En una realización de este tipo, la pantalla de pago sustituta posibilita que el titular introduzca datos de PIN, datos de firma, datos biométricos, o similares.

Aunque no se muestra en la Figura 6, la PSL puede invocarse también por una llamada de programa. En una implementación de este tipo, un componente de software en el terminal de POS puede hacer una llamada de función usando, por ejemplo, una biblioteca dinámica enlazada (DLL), que invoca la PSL.

La Figura 7 es un diagrama de flujo que ilustra una realización de un método 300 para encriptar datos de pago. El método 300 puede realizarse por cualquiera de los sistemas de POS anteriormente descritos y como parte del proceso de la Figura 3 o 4. En particular, el método 300 se realiza por la SSA en un ejemplo. Ventajosamente, el método 300 posibilita que se aseguren transacciones de débito en línea. En algunas implementaciones, la expresión "débito en línea" indica usar un PIN para completar una transacción de débito, y la expresión "débito fuera de línea" hace referencia a usar una firma para completar una transacción de débito. El débito en línea a menudo se denomina coloquialmente como una transacción de "débito", y el "débito fuera de línea" a menudo se denomina como una transacción de "crédito".

En 304, el método 300 encripta datos de pago con un cifrado "que no puede desencriptarse". En un ejemplo, los datos no pueden desencriptarse en el punto de venta, por ejemplo, en el terminal de POS o servidor de POS. Sin embargo, los datos pueden desencriptarse en una pasarela u otro servidor remoto.

En 306, el método 300 encripta los datos de pago con un cifrado que puede desencriptarse. En un ejemplo, los datos pueden desencriptarse en el punto de venta, por ejemplo, en el terminal de POS o servidor de POS. El método 300 en una implementación encripta los datos con el cifrado que puede desencriptarse al mismo tiempo o sustancialmente

al mismo tiempo que el método 300 que encripta los datos con el cifrado que no puede desencriptarse.

El método 300 a continuación determina si está teniendo lugar una transacción de débito en línea en 308. Si la transacción no es de débito en línea (por ejemplo, es una transacción de débito fuera de línea, de crédito o de tarjeta de regalo), el método 300 destruye la versión que puede desencriptarse en 310. Sin embargo, si la transacción es de débito en línea, el método 300 continúa para desencriptar la versión que puede desencriptarse de los datos de pago en 312. La versión que puede desencriptarse se destruye por la SSA, aunque en un ejemplo alternativo, la PSL realiza esta función. Posteriormente, el método 300 encripta el PIN usando los datos de pago desencriptados para crear un bloque de PIN encriptado en 314. Una vez que se crea el bloque de PIN encriptado, el método 300 destruye la versión que puede desencriptarse de los datos de pago en 316. Como anteriormente, la versión que puede desencriptarse se destruye por la SSA, pero la PSL puede realizar también esta función. Además, en un ejemplo alternativo, el método 300 puede aplicarse a una tarjeta de crédito, tarjeta de regalo, u otra tarjeta que tenga un PIN, en lugar de una tarjeta de débito.

Una implementación de ejemplo del método 300 es como sigue. Una SSA encripta datos de pago recibidos de una PSL con un cifrado "que no puede desencriptarse" en 304 y un cifrado que puede desencriptarse en 306. La SSA determina si la transacción es de débito en línea en 308. Si la transacción no es de débito en línea, la SSA borra la versión que puede desencriptarse de los datos en 310. La SSA puede borrar los datos tras la detección de una transacción de débito no en línea, o la SSA puede emplear un periodo de tiempo de espera (por ejemplo, 30 segundos), después del cual la versión que puede desencriptarse se destruirá automáticamente. Además, la versión que puede desencriptarse puede almacenarse en memoria volátil (memoria que se borra en el apagado), tal como en memoria de acceso aleatorio (RAM). En un ejemplo, el periodo de tiempo de espera se ajusta para equilibrar fiabilidad transaccional con seguridad. Como alternativa, la SSA determina que la transacción es de débito en línea y envía la versión que puede desencriptarse a la PSL, que desencripta la versión que puede desencriptarse de los datos de pago en 312. La PSL a continuación proporciona los datos de pago desencriptados al teclado de pin, que en 314 encripta el PIN usando alguno o todos los datos de pago (por ejemplo, el PAN o datos de rastreo completos). Una vez que se encripta el PIN o después de un periodo de tiempo de espera, la SSA destruye (borra de manera permanente la única copia de) la versión que puede desencriptarse de los datos de pago almacenados en el servidor de POS en 316. Además, si una copia de la versión que puede desencriptarse se almacenan en el terminal de POS, la PSL también destruye estos datos.

Algunos negocios no aceptan transacciones de débito en línea o cualesquiera transacciones de débito. En estos negocios, el método 300 puede configurarse para proporcionar únicamente una versión que no puede desencriptarse de los datos de pago. Por lo tanto, puede no haber necesidad almacenar una versión que puede desencriptarse.

Volviendo a la Figura 8, se muestran diversos formatos de datos de pago, algunos o todos los cuales se generan durante el flujo de proceso anteriormente descrito bajo cualquiera de las Figuras 3 o 4.

La Figura 8 ilustra datos 410 reales, presentados originalmente por el titular. Estos datos 410 reales se encriptan por una PSL y se vuelven datos 430 encriptados. Posteriormente, una SSA desencripta los datos 430 encriptados y sustituye los datos 410 reales por datos 450 falsos. Además, la SSA re-encripta los datos 410 reales para generar datos 460 re-encriptados. La SSA combina los datos 450 falsos y los datos 460 re-encriptados para crear datos 470 combinados, que la SSA transmite a una pasarela.

Los diversos formatos de datos de pago mostrados se representan como datos de rastreo. Los datos 410 reales están contenidos en una pasada magnética en la tarjeta de pago. Esta pasada magnética incluye una o más "pistas" de datos. Muchas tarjetas de débito y crédito tienen tres pistas de datos, que se denominan típicamente como "pista 1", "pista 2", y "pista 3". De estas pistas, la pista 2 a menudo se usa por los distribuidores para obtener datos de pago de la tarjeta de pago. Se muestra un ejemplo de los datos de la pista 2 en la Figura 8 como los datos 310 reales.

Los datos 310 reales incluyen un centinela 412 de inicio, representado por el carácter ";''. El centinela 412 de inicio se usa, por ejemplo, mediante software de análisis para indicar el inicio de los datos de la pista 2. Después del centinela 412 de inicio, se muestra un PAN 414. El PAN 414 representado incluye 16 dígitos. En ejemplos alternativos, se incluyen más o menos dígitos en el PAN 414.

Después del PAN 414, se muestra un separador 416 de campo, indicado por el carácter "=". El separador 416 de campo posibilita que el software de análisis distinga entre el PAN 414 y datos que siguen el PAN 416. Después del separador 416 de campo, se muestran los datos 418 auxiliares. Los datos 418 auxiliares pueden incluir la fecha de caducidad de la tarjeta, el PIN de la tarjeta y otros datos discrecionales determinados por el emisor de la tarjeta. En el ejemplo representado, los primeros cuatro dígitos de los datos 418 auxiliares se reservan para la fecha de caducidad de la tarjeta usando el formato AAMM ("0101"). Un centinela 420 de fin ("?") que sigue los datos 418 auxiliares para marcar el fin de la pista.

En ciertos ejemplos, los datos de la pista 1 (no mostrados) se usan en lugar de o además de los datos de la pista 2. Un posible formato de los datos de la pista 1 puede ser el siguiente: "% B PAN ^ Nombre de titular ^ datos auxiliares ?". Al igual que los datos de la pista 2, los datos de la pista 1 incluyen los centinelas de inicio y fin ("%" y "?"), uno o

más separadores de campo ("^"), el PAN, y datos auxiliares. Los datos de la pista 1 también incluyen un código de formato ("B"), que puede variar, y el nombre del titular. Aunque el resto de la Figura 8 describe un ejemplo específico que usa los datos de la pista 2, los datos de la pista 1 pueden usarse también de manera intercambiable o con ligeras modificaciones. Análogamente, aunque no se muestra, en algunas implementaciones pueden usarse también los datos de la pista 3.

Durante el flujo de proceso descrito bajo las Figuras 3 y 4 anteriores, los datos 410 reales se encriptan por una PSL para generar datos 430 encriptados. Los datos 430 encriptados incluyen un bloque 432 de representaciones alfanuméricas y/o simbólicas de los datos 410 reales.

Los datos 430 encriptados se desencriptan por la SSA, y la SSA sustituye los datos 410 reales por datos 450 falsos. En un ejemplo, los datos 450 falsos parecen sustancialmente similares a los datos 410 reales. Puesto que los datos 450 falsos son similares (en el mismo formato que) los datos 410 reales, un terminal de POS y servidor de POS pueden procesar los datos 450 falsos como si fueran los datos 410 reales sin tener conocimiento del procesamiento de los datos 450 falsos. Por lo tanto, en un ejemplo los datos 450 falsos tienen un formato compatible con pasada de tarjeta.

En el ejemplo representado, los datos 450 falsos son una versión modificada de los datos 410 reales. Los datos 450 falsos incluyen los mismos centinelas 412, 420 de inicio y fin y el mismo separador 416 de campo. Sin embargo, un PAN 452 de los datos 450 falsos difiere del PAN 414 de los datos 414 reales. Además, los datos 454 auxiliares de los datos 450 falsos difieren de los datos 418 auxiliares de los datos 410 reales.

El PAN 452 de los datos 450 falsos en una implementación mantiene los primeros cuatro dígitos ("1234") y los últimos cuatro dígitos ("3456") del PAN 414 de los datos 410 reales. Entre los primeros cuatro y los últimos cuatro dígitos, los dígitos de los datos 410 reales se sustituyen por dígitos 456 falsos, por ejemplo, "00000000" en el ejemplo representado. Además, los datos 454 auxiliares de los datos 450 falsos incluyen datos falsos en el ejemplo representado. En el ejemplo representado, estos datos falsos sustituyen completamente los datos 418 auxiliares de los datos 410 reales. Como alternativa, los datos 454 auxiliares no incluyen datos falsos.

Los datos 450 falsos para una tarjeta de pago particular son únicos y distintos de otros datos de pago falsos 450 que corresponden a otras tarjetas de pago. En un ejemplo, esta unicidad se consigue combinando los dígitos 456 falsos entre los primeros y cuatro últimos dígitos del PAN 452. Además, los datos 454 auxiliares pueden generarse para proporcionar datos 450 falsos únicos.

Los dígitos 456 falsos pueden generarse aleatoriamente. Como alternativa, los dígitos 456 falsos se generan incrementalmente, donde a cada tarjeta de pago sucesiva presentada en el POS se le proporciona un número sucesivo en una secuencia. Por ejemplo, los dígitos 456 falsos pueden incrementarse de 11111111 a 22222222 y así sucesivamente hasta 99999999. Además, los dígitos 456 falsos pueden generarse a partir de un algoritmo que usa la fecha, hora y/o el origen de la transacción para derivar un conjunto de dígitos. En otra implementación, los dígitos 456 falsos se generan de acuerdo con otro tipo de algoritmo o una combinación de los algoritmos anteriormente descritos. Análogamente, los datos 454 auxiliares falsos pueden generarse aleatoria, secuencial o algorítmicamente.

En otro ejemplo, los datos 450 falsos se generan de manera que los datos 450 falsos fallan en el algoritmo de módulo 10 de Luhn ("la prueba de Luhn"), como se describe en la Patente de Estados Unidos N. º 2.950.048, titulada "Computer for Verifying Numbers". La prueba Luhn detecta un número de tarjeta válido realizando una suma de comprobación de los dígitos del número de tarjeta. Los datos 450 falsos por lo tanto pueden generarse de manera que una suma de comprobación de los dígitos de los datos 450 falsos indica que los datos 450 falsos son un número de tarjeta de pago inválido. En consecuencia, los datos 450 falsos en este ejemplo no pueden usarse de manera fraudulenta como un número de tarjeta válido.

Los datos 450 falsos pueden generarse para fallar la prueba de Luhn en una diversidad de maneras. En un ejemplo, en primer lugar se generan los datos 450 falsos que pasan la prueba de Luhn. A continuación, se modifican los datos 450 falsos de modo que ya no pasan más la prueba de Luhn, por ejemplo, cambiando un dígito en los datos 450 falsos. Por ejemplo, si uno de los dígitos en los datos 450 falsos es un 5, el algoritmo podría sustituir el 5 con cualquiera de los números 0-4 o 6-9, provocando que el PAN falso fallara la prueba de Luhn.

Además o como alternativa a la prueba de Luhn, pueden usarse intervalos inválidos de números de tarjeta para generar los datos 450 falsos. Por ejemplo, pueden designarse diferentes intervalos de números de tarjeta inválidos por diferente asociación de tarjetas (por ejemplo, Visa, American Express, o similares); puede a continuación usarse un algoritmo de generación de datos falsos que asegura que todos los números de tarjeta falsos generados para un tipo de tarjeta particular (por ejemplo, Visa) caen dentro del intervalo inválido correspondiente. En un ejemplo, al menos una porción de los datos 450 falsos se deriva o selecciona de esta manera a partir de un intervalo de números de tarjeta inválidos creados por una o más asociaciones de tarjetas. Por ejemplo, si una asociación de tarjeta usa el intervalo 4000000000000000 a 4999999999999999 para números de PAN válidos, al menos una porción de los datos 450 falsos podría tomar un número de 0000000000000000 a 3999999999999999 o de 5000000000000000 a 9999999999999999. Ventajosamente, los datos 450 falsos derivados de estos intervalos en ciertas realizaciones no pueden usarse para autorizaciones fraudulentas. Además, en una implementación, los datos 450 falsos pueden

derivarse de cualquier intervalo inválido de números de tarjeta y también pueden generarse para fallar la prueba de Luhn.

Los datos 450 falsos generados para fallar la prueba de Luhn o generados a partir de un intervalo inválido de números de tarjeta pueden usarse beneficiosamente como un testigo para transacciones adicionales. En un ejemplo, los datos 450 falsos se usan directamente como un testigo, o como alternativa, se deriva un testigo de los datos 450 falsos. En un ejemplo, el testigo incluye tres partes. Estas partes pueden incluir alguna porción de los primeros cuatro dígitos del PAN, seguido por siete dígitos de datos falsos, seguido por los últimos cuatro dígitos del PAN. Puesto que el testigo es un número de tarjeta inválido, el testigo puede usarse en ciertos sistemas de POS complejos para transacciones adicionales o recurrentes. Además, esta implementación de un testigo puede permitir mayor flexibilidad para un procesamiento de transacción posterior, de manera que el testigo puede usarse para procesar transacciones posteriores de una manera similar a modelos de generación de testigos existentes.

Algunos terminales y/o servidores de POS pueden cambiarse para desactivar el uso de la prueba de Luhn para facilitar usar datos 450 falsos que fallan la prueba de Luhn. Como algunos fabricantes de terminal y/o servidor de POS tienen la prueba de Luhn activada o una base de tipo de pago (por ejemplo, tipo de pago de tarjeta de crédito, tipo de pago de tarjeta de débito, o similares), esta característica particular puede desactivarse para alguno o todos los tipos de pago aceptados por un comerciante particular. Por lo tanto, en diversos ejemplos, los datos 450 falsos tienen un formato compatible con pasada de tarjeta que puede procesarse por el sistema de POS, pero los datos 450 falsos son un número de tarjeta inválido.

Debido a que los primeros y últimos cuatro dígitos del PAN 414 se mantienen en el PAN falso 452 en algunas variaciones, la combinación de dígitos definidos de manera aleatoria, secuencial o algorítmica y los primeros y últimos cuatro dígitos del PAN 452 será probable que sean únicos a partir de los datos 450 falsos generados para otras tarjetas de pago. Si se genera un número no único, en una realización la SSA re-genera los datos 450 falsos hasta que se halla un número único.

Los dígitos 456 falsos pueden también estar vinculados a una transacción particular. Por lo tanto, en un ejemplo, puede asignarse una tarjeta de pago único en múltiples transacciones a un único conjunto de datos 450 falsos para cada transacción. Como alternativa, transacciones sucesivas usan los mismos datos 450 falsos.

Aunque se ha descrito un ejemplo de los datos 450 falsos, los datos 450 falsos pueden implementarse de otras maneras. Por ejemplo, pueden mantenerse menos o más que los primeros y últimos cuatro dígitos del PAN 414 real, o pueden mantenerse porciones de los datos 418 auxiliares adicionales. Además, los datos 418 auxiliares pueden falsificarse en datos 454 auxiliares falsos de manera aleatoria, secuencial o algorítmica. Además, en un ejemplo, uno o más de los centinelas 412, 420 de inicio o final o del separador 416 de campo se sustituyen por datos falsos. Además, aunque se han usado números para representar datos falsos, en una realización, los datos 450 falsos incluyen caracteres alfanuméricos o simbólicos falsos.

Los datos 450 falsos o porciones de los mismos (por ejemplo, los dígitos 456 falsos) no pueden transformarse en los datos 410 reales en algunas realizaciones puesto que se generan por un proceso aleatorio, secuencia o algoritmo que no está basado en los datos 410 reales. Por lo tanto, los datos 450 falsos de tales realizaciones llevan poca o ninguna relación con los datos 410 reales. Los datos 450 falsos de tales realizaciones están correlacionados con los datos 410 reales únicamente por la SSA que combina los datos 410 falsos y re-encriptados 460 juntos para su transmisión a la pasarela. Por lo tanto, cuando la SSA borra los datos 460 re-encriptados después de la transmisión, únicamente la pasarela conoce los datos 410 reales y a qué datos 410 reales corresponden los datos 450 falsos. Por lo tanto, los datos 450 falsos de ciertas realizaciones ayudan a asegurar el sistema de POS.

La Figura 8 también representa los datos 460 re-encriptados. Estos datos 460 se generan por la SSA después de que la SSA desencripta los datos 430 encriptados recibidos de la PSL. Aunque únicamente se muestra un bloque de datos, los datos 460 re-encriptados pueden realmente ser dos bloques de datos - un bloque de datos que no puede desencriptarse y un bloque de datos que puede desencriptarse (véase la Figura 7). Los dos bloques de datos pueden tener diferentes valores.

La SSA combina los datos 450 falsos y los datos 460 re-encriptados en los datos 470 combinados. La SSA puede usar cualquiera del bloque de datos que no puede desencriptarse o que puede desencriptarse para crear los datos 470 combinados. Aunque los datos combinados se forman por concatenación en este ejemplo, puede usarse cualquier método de combinación de los datos 450 falsos y re-encriptados 460 con la condición de que el método sea conocido para la pasarela. La SSA proporciona los datos 470 combinados a la pasarela, que desencripta los datos 460 re-encriptados almacenados en los datos 470 combinados para recuperar los datos 410 reales. Aunque no se muestra, la pasarela puede re-encriptar también los datos 410 reales en un formato que puede desencriptarse por la entidad de autorización (por ejemplo, banco emisor). La pasarela puede en su lugar no desencriptar los datos 460 re-encriptados, sino en su lugar pasar los datos 460 re-encriptados directamente a la entidad de autorización.

Volviendo a la Figura 9, se muestran ejemplos de un método 500 para obtener autorizaciones o liquidaciones incrementales. Los datos de pago a menudo se usan para realizar autorizaciones o liquidaciones incrementales. Por

ejemplo, en el entorno de restaurante, la tarjeta de pago autoriza en primer lugar la cantidad de la factura. Sin embargo, de manera frecuente el comerciante añade cargos incrementales, tales como propinas y cuentas a la factura después de que el titular ha marchado. Para completar la transacción incremental, el comerciante mantiene los datos de pago.

De manera similar, en las industrias de alojamiento y alquiler, se usan autorizaciones incrementales. Por ejemplo, los negocios de hoteles y alquiler de coches usan autorizaciones de tarjeta de pago para hacer reservas. Almacenar datos de pago posibilita que los hoteles y negocios de alquiler de coche facturen múltiples elementos a una única factura. Los clientes de hotel a menudo desean y esperan la capacidad de facturar artículos a su habitación de la tienda de regalos, restaurante, spa, y similares. En algunos casos, puede no ser siempre posible solicitar que el titular presente una tarjeta para cubrir el coste de los incidentes. El titular puede ya haber pagado, por ejemplo, antes del descubrimiento de un mini bar agotado, o puede haber dicho que devolvería el tanque de un coche lleno de gasolina, pero de hecho no lo hizo.

Además, el pedido por correo, pedido de teléfono, y negocios en línea a menudo operan usando un modelo de "reserva y envío". En este modelo, se realiza el pedido, pero no se cobra a la tarjeta de crédito hasta que el pedido se envía realmente. En estos casos, se mantienen datos de pago hasta que se envíe al pedido y se cobra la tarjeta la cantidad del pedido. Además, los comerciantes que cobran afiliación mensual, tales como spas, clubs y gimnasios, también almacenan los datos de pago para procesar estos cobros mensuales.

Por consiguiente, la Figura 9 ilustra un método 500 para obtener autorizaciones o liquidaciones incrementales. En 502, el método obtiene datos de pago. Los datos de pago pueden obtenerse, por ejemplo, por la PSL. El método 500 a continuación almacena datos 504 falsos en lugar de los datos de pago. En un ejemplo, la aplicación de servidor de POS almacena datos falsos proporcionados por la aplicación de terminal de POS como si fueran los datos de pago reales. En 506, el método obtiene una autorización inicial o liquidación 506 usando los datos falsos. Esta etapa puede incluir las subetapas de solicitar una autorización o liquidación usando la aplicación de terminal de POS y/o SSA, recibir la autorización o liquidación con la pasarela, y recibir la respuesta de autorización o liquidación de la pasarela en la SSA.

Posteriormente, el método 500 determina en 508 si ha de realizarse una autorización incremental o una liquidación. En un ejemplo, esta determinación se hace por la aplicación de terminal de POS. Si no hay una autorización o liquidación de este tipo, el método finaliza. De otra manera, el método 500 usa los datos falsos almacenados en 510 para obtener una autorización incremental o liquidación retardada usando, por ejemplo, la SSA para solicitar la autorización o liquidación. Puesto que el método 500 usa datos falsos para realizar las autorizaciones o liquidaciones adicionales, no necesitan almacenarse datos de pago sensibles en la localización del comerciante para realizar autorizaciones o liquidaciones adicionales. Como resultado, el método 500 aumenta la seguridad de transacciones de tarjeta de pago.

Además de los ejemplos anteriormente descritos, algunos o todos los diversos sistemas y métodos descritos en el presente documento pueden emplearse con un almacén en línea a través de la Internet. Por ejemplo, el punto de venta puede incluir un programa de carrito de la compra en la tienda en línea, y la tienda en línea puede procesar toda o una porción de una transacción usando datos falsos. Además, al menos una porción de los sistemas y métodos descritos en el presente documento puede implementarse en un centro de llamadas telefónicas. Por ejemplo, un operador puede tomar datos de pago de un comerciante a través del teléfono e introducir los datos de pago en un terminal de POS seguro, que realiza toda o una porción de la transacción usando datos falsos.

Además, aunque el terminal de POS y el servidor de POS se han descrito como dispositivos separados, en ciertos ejemplos el terminal de POS y el servidor de POS son un único dispositivo físico, o las funciones del terminal de POS y el servidor se realizan por un único dispositivo. Como resultado, en un ejemplo se implementa alguna o todas funciones del terminal de POS y el servidor, excepto que no se usa red para comunicar entre el terminal de POS y el servidor. Adicionalmente, alguna o todas las funciones del terminal de POS pueden realizarse por el servidor de POS, y viceversa. Pueden emplearse también otras implementaciones, como se entenderá por los expertos en la materia.

Los expertos en la materia apreciarán que los diversos bloques lógicos ilustrativos, módulos, componentes, y etapas de proceso descritos en relación con las realizaciones desveladas en el presente documento pueden implementarse como hardware electrónico, software informático, o combinaciones de ambos. Para ilustrar de manera clara esta intercambiabilidad de hardware y software, se han descrito diversos componentes ilustrativos, bloques, componentes, y etapas anteriormente en general en términos de su funcionalidad. Si tal funcionalidad se implementa como hardware o software depende de la aplicación particular y restricciones de diseño impuestas en el sistema global. Los expertos en la materia pueden implementar la funcionalidad descrita en manera variable para cada aplicación particular, pero tales decisiones de implementación no deberían interpretarse como que provocan un alejamiento del alcance de la presente invención.

REIVINDICACIONES

1. Un método de aseguración de transacciones de tarjeta de pago en un punto de venta (POS) en un sistema de procesamiento de tarjeta de pago, comprendiendo el sistema un terminal (30) de POS y un servidor (36) de POS en comunicación con el terminal de POS a través de una red, comprendiendo el terminal (30) de POS un ordenador (34) de anfitrión y un dispositivo (28) de entrada de tarjeta, teniendo el ordenador anfitrión una aplicación (38) de terminal de POS y una capa (40) de seguridad de POS instalada en el mismo, teniendo el servidor de POS una aplicación (46) de servidor de POS y una aplicación (48) de seguridad de servidor instalada en el mismo, la aplicación (46) de servidor de POS en comunicación con la aplicación (38) de terminal de POS para procesar transacciones de tarjeta de pago, la aplicación (48) de seguridad de servidor en comunicación con la capa (40) de seguridad de POS a través de un canal (44) seguro en la red, comprendiendo el método:

la capa (40) de seguridad de POS:

interceptar datos de pago reales recibidos del dispositivo de entrada de tarjeta cuando un usuario inicia una transacción de tarjeta de pago mediante la cual se evita que los datos de pago reales alcancen la aplicación (38) de terminal de POS; y
enviar los datos de pago reales a la aplicación (48) de seguridad de servidor a través del canal (44) seguro;

la aplicación (48) de seguridad de servidor:

recibir los datos de pago reales de la capa (40) de seguridad de POS a través del canal seguro;
generar datos de pago falsos sustituyendo toda o una porción de los datos de pago reales por datos de pago falsos; y
transmitir los datos de pago falsos a través del canal (44) seguro a la capa (40) de seguridad de POS;

la capa (40) de seguridad de POS:

recibir los datos de pago falsos de la aplicación (48) de seguridad de servidor a través del canal (44) seguro; y
pasar los datos de pago falsos a la aplicación de terminal de POS para su uso en lugar de los datos de pago reales;

la aplicación (38) de terminal de POS:

recibir los datos de pago falsos de la capa (40) de seguridad de POS; y
transmitir los datos de pago falsos a través de la red a la aplicación (48) de servidor de POS;

la aplicación (46) de servidor de POS:

recibir los datos de pago falsos a través de la red de la aplicación (38) de terminal de POS;
procesar los datos de pago falsos como si fueran datos de pago reales mediante los cuales los datos de pago falsos se almacenan en una base de datos (50) en lugar de los datos de pago reales; y
transmitir los datos de pago falsos a la aplicación (48) de seguridad de servidor para procesamiento de pago;

la aplicación (48) de seguridad de servidor:

recibir los datos de pago falsos de la aplicación (46) de servidor de POS; y
usar los datos de pago falsos para procesar la transacción de tarjeta de pago transmitiendo una solicitud de autorización a una pasarela (52) de pago, comprendiendo la solicitud de autorización los datos de pago falsos y los datos de pago reales.

2. El método de la reivindicación 1, que comprende adicionalmente generar la aplicación (48) de seguridad de servidor los datos de pago falsos usando un algoritmo que garantiza sustancialmente que los datos de pago falsos no representen datos de tarjeta válidos.

3. Un método de aseguración de transacciones de tarjeta de pago en un punto de venta (POS) en un sistema de procesamiento de tarjeta de pago, comprendiendo el sistema un terminal (30) de POS y un servidor (36) de POS en comunicación con el terminal de POS a través de una red, comprendiendo el terminal (30) de POS un ordenador (34) de anfitrión y un dispositivo (28) de entrada de tarjeta, teniendo el ordenador anfitrión una aplicación (38) de terminal de POS y una capa (40) de seguridad de POS instalada en el mismo, teniendo el servidor de POS una aplicación (46) de servidor de POS y una aplicación (48) de seguridad de servidor instalada en el mismo, la aplicación (46) de servidor de POS en comunicación con la aplicación (38) de terminal de POS para procesar transacciones de tarjeta de pago, la aplicación (48) de seguridad de servidor en comunicación con la capa (40) de seguridad de POS a través de un canal (44) seguro en la red, comprendiendo el método:

la capa (40) de seguridad de POS:

interceptar datos de pago reales recibidos del dispositivo de entrada de tarjeta cuando un usuario inicia una transacción de tarjeta de pago mediante la cual se evita que los datos de pago reales alcancen la aplicación (38) de terminal de POS;
generar datos de pago falsos sustituyendo toda o una porción de los datos de pago reales por datos de pago falsos; y
transmitir los datos de pago reales y los datos de pago falsos a través del canal (44) seguro a la aplicación (48) de seguridad de servidor;

la aplicación (48) de seguridad de servidor:
recibir datos de pago reales y los datos de pago falsos de la capa (40) de seguridad de POS a través del canal (44) seguro;
la capa (40) de seguridad de POS:
pasar los datos de pago falsos a la aplicación (38) de terminal de POS para su uso en lugar de los datos de pago reales;
la aplicación (38) de terminal de POS:

recibir los datos de pago falsos de la capa (40) de seguridad de POS; y
transmitir los datos de pago falsos a través de la red a la aplicación (48) de servidor de POS;

la aplicación (46) de servidor de POS:

recibir los datos de pago falsos a través de la red de la aplicación (38) de terminal de POS;
procesar los datos de pago falsos como si fueran datos de pago reales mediante los cuales los datos de pago falsos se almacenan en una base de datos (50) en lugar de los datos de pago reales; y transmitir los datos de pago falsos a la aplicación (48) de seguridad de servidor para procesamiento de pago;

la aplicación (48) de seguridad de servidor:

recibir los datos de pago falsos de la aplicación (46) de servidor de POS; y
usar los datos de pago falsos para procesar la transacción de tarjeta de pago transmitiendo una solicitud de autorización a una pasarela (52) de pago, comprendiendo la solicitud de autorización los datos de pago falsos y los datos de pago reales.

4. Un sistema de procesamiento de tarjeta de pago para asegurar transacciones de tarjeta de pago en un punto de venta (POS), comprendiendo el sistema un terminal (30) de POS y un servidor (36) de POS en comunicación con el terminal de POS a través de una red, comprendiendo el terminal (30) de POS un ordenador (34) de anfitrión y un dispositivo (28) de entrada de tarjeta, teniendo el ordenador anfitrión una aplicación (38) de terminal de POS y una capa (40) de seguridad de POS instalada en el mismo, teniendo el servidor de POS una aplicación (46) de servidor de POS y una aplicación (48) de seguridad de servidor instalada en el mismo, la aplicación (46) de servidor de POS en comunicación con la aplicación (38) de terminal de POS para procesar transacciones de tarjeta de pago, la aplicación (48) de seguridad de servidor en comunicación con la capa (40) de seguridad de POS a través de un canal (44) seguro en la red, en el que el sistema de procesamiento de tarjeta de pago está configurado para realizar el método de cualquier reivindicación anterior.

5. Un medio legible por ordenador que tiene almacenado en el mismo una capa (40) de seguridad de punto de venta (POS) que está configurada para instalarse en un terminal (30) de POS de un sistema de procesamiento de tarjeta de pago de acuerdo con la reivindicación 4 cuando depende de la reivindicación 1 o la reivindicación 2, en el que el terminal (30) de POS ejecuta una aplicación (38) de terminal de POS y en el que la capa (40) de seguridad de POS comprende instrucciones ejecutables que provocan a la capa (40) de seguridad de POS:

interceptar datos de pago reales recibidos del dispositivo de entrada de tarjeta cuando un usuario inicia una transacción de tarjeta de pago mediante la cual se evita que los datos de pago reales alcancen la aplicación (38) de terminal de POS;
enviar los datos de pago reales a la aplicación (48) de seguridad de servidor a través del canal (44) seguro; y
recibir los datos de pago falsos a través del canal (44) seguro de la aplicación (48) de seguridad de servidor; y
pasar los datos de pago falsos a la aplicación de terminal de POS para su uso en lugar de los datos de pago reales.

6. Un medio legible por ordenador que tiene almacenado en el mismo una capa (40) de seguridad de punto de venta (POS) que está configurada para instalarse en un terminal (30) de POS de un sistema de procesamiento de tarjeta de pago de acuerdo con la reivindicación 4 cuando depende de la reivindicación 3, en el que el terminal (30) de POS ejecuta una aplicación (38) de terminal de POS y en el que la capa (40) de seguridad de POS comprende instrucciones ejecutables que provocan a la capa (40) de seguridad de POS:

interceptar datos de pago reales recibidos del dispositivo de entrada de tarjeta cuando un usuario inicia una transacción de tarjeta de pago mediante la cual se evita que los datos de pago reales alcancen la aplicación (38)

de terminal de POS;
generar datos de pago falsos sustituyendo toda o una porción de los datos de pago reales por datos de pago falsos;
transmitir los datos de pago reales y los datos de pago falsos a través del canal (44) seguro a la aplicación (48) de seguridad de servidor;
pasar los datos de pago falsos a la aplicación (38) de terminal de POS para su uso en lugar de los datos de pago reales.

7. Un medio legible por ordenador que tiene almacenado en el mismo una aplicación (48) de seguridad de servidor que está configurada para instalarse en un servidor de punto de venta (POS) de un sistema de procesamiento de tarjeta de pago de acuerdo con la reivindicación 4 cuando depende de la reivindicación 1 o la reivindicación 2, en el que el servidor de POS ejecuta una aplicación (46) de servidor de POS y en el que la aplicación de seguridad de servidor comprende instrucciones ejecutables que provocan a la aplicación (48) de seguridad de servidor:

recibir los datos de pago reales de la capa (40) de seguridad de POS a través del canal (44) seguro;
generar datos de pago falsos sustituyendo toda o una porción de los datos de pago reales por datos de pago falsos;
transmitir los datos de pago falsos a través del canal (44) seguro a la capa (40) de seguridad de POS;
recibir los datos de pago falsos de la aplicación (46) de servidor de POS; y
usar los datos de pago falsos para procesar la transacción de tarjeta de pago transmitiendo una solicitud de autorización a una pasarela (52) de pago, comprendiendo la solicitud de autorización los datos de pago falsos y los datos de pago reales.

8. Un medio legible por ordenador que tiene almacenado en el mismo una aplicación (48) de seguridad de servidor que está configurada para instalarse en un servidor de punto de venta (POS) de un sistema de procesamiento de tarjeta de pago de acuerdo con la reivindicación 4 cuando depende de la reivindicación 3, en el que el servidor de POS ejecuta una aplicación (46) de servidor de POS y en el que la aplicación de seguridad de servidor comprende instrucciones ejecutables que provocan a la aplicación (48) de seguridad de servidor:

recibir datos de pago reales y los datos de pago falsos de la capa (40) de seguridad de POS a través del canal (44) seguro;
recibir los datos de pago falsos de la aplicación (46) de servidor de POS; y
usar los datos de pago falsos para procesar la transacción de tarjeta de pago transmitiendo una solicitud de autorización a una pasarela (52) de pago, comprendiendo la solicitud de autorización los datos de pago falsos y los datos de pago reales.

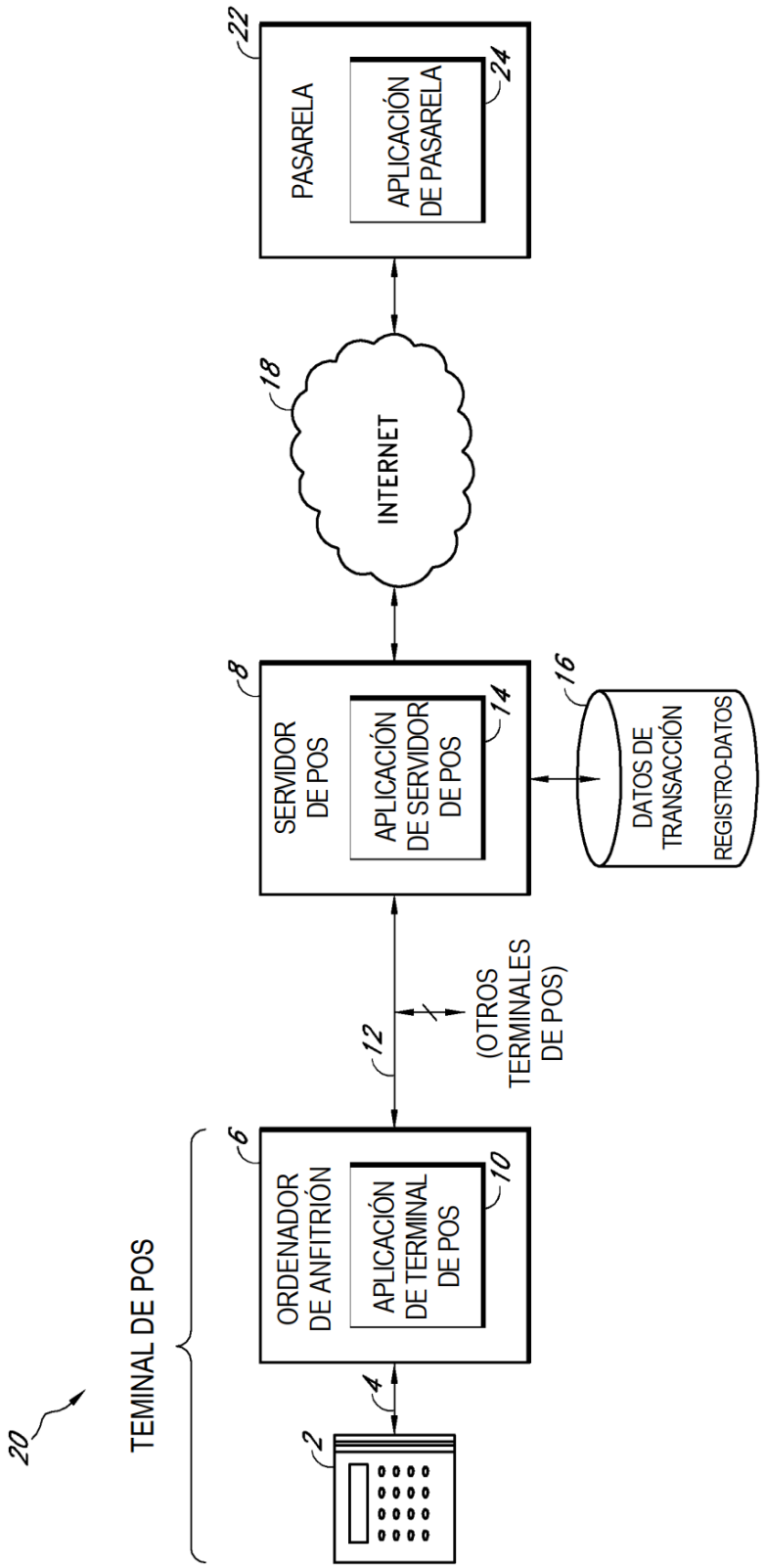


FIG. 1
(TÉCNICA ANTERIOR)

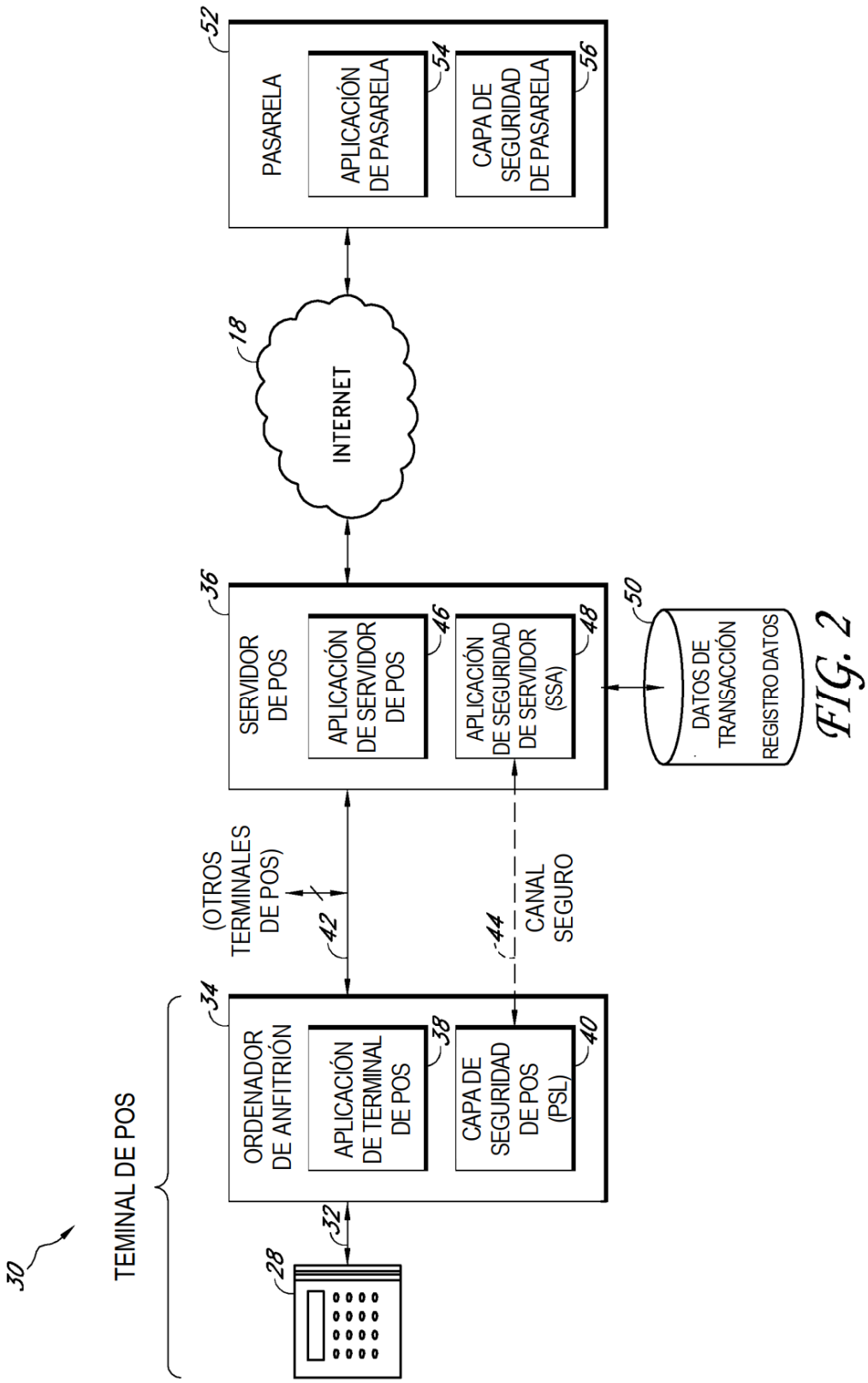
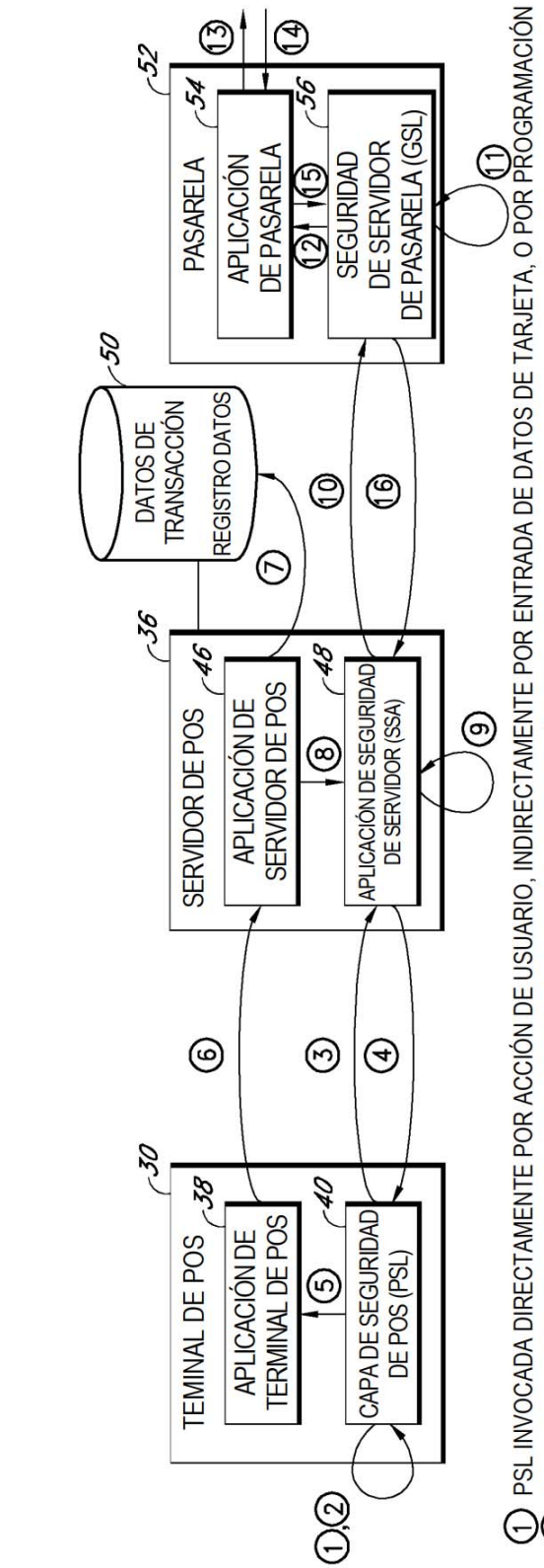

30
TEMINAL DE POS
ORDENADOR DE ANFITRIÓN
34
APLICACIÓN DE TERMINAL DE POS
38
CAPA DE SEGURIDAD DE POS (PSL)
40
32
28
(OTROS TERMINALES DE POS)
42
CANAL SEGURO
44
SERVIDOR DE POS
36
APLICACIÓN DE SERVIDOR DE POS
46
APLICACIÓN DE SEGURIDAD DE SERVIDOR (SSA)
48
DATOS DE TRANSACCIÓN REGISTRO DATOS
50
INTERNET
18
PASARELA
52
APLICACIÓN DE PASARELA
54
CAPA DE SEGURIDAD DE PASARELA
56

FIG. 2



① PSL INVOCADA DIRECTAMENTE POR ACCIÓN DE USUARIO, INDIRECTAMENTE POR ENTRADA DE DATOS DE TARJETA, O POR PROGRAMACIÓN
② PSL VISUALIZA INTERFAZ DE USUARIO DE PAGO Y CAPTURA INFORMACIÓN DE PAGO
③ PSL ENVÍA INFORMACIÓN DE PAGO CAPTURADA A SSA A TRAVÉS DE CANAL SEGURO
④ SSA DEVUELVE DATOS DE PAGO FALSOS
⑤ PSL PASA DATOS DE PAGO FALSOS A APLICACIÓN DE TERMINAL DE POS
⑥ APLICACIÓN DE TERMINAL DE POS PASA DATOS DE PAGO FALSOS A APLICACIÓN DE SERVIDOR DE POS
⑦ APLICACIÓN DE SERVIDOR DE POS REGISTRA TRANSACCIÓN CON DATOS DE PAGO FALSOS EN UNA BASE DE DATOS
⑧ APLICACIÓN DE SERVIDOR DE POS ENVÍA MENSAJE DE SOLICITUD DE PAGO A SSA
⑨ SSA MODIFICA MENSAJE DE SOLICITUD DE PAGO COMBINANDO DATOS DE PAGO FALSOS CON DATOS DE PAGO ENCRIPTADOS
⑩ SSA ENVÍA DATOS DE PAGO COMBINADOS A GSL
⑪ GSL DESENCRIPTA LOS DATOS DE PAGO ENCRIPTADOS PARA RECUPERAR LOS DATOS DE PAGO REALES
⑫ GSL PASA LOS DATOS DE PAGO A APLICACIÓN DE PASARELA
⑬ APLICACIÓN DE PASARELA TRANSMITE DATOS DE PAGO A PROCESADOR Y MENSAJE DE SOLICITUD DE PAGO A PROCESADOR
⑭ PROCESADOR DEVUELVE DATOS DE PAGO Y RESPUESTA DE SOLICITUD DE PAGO A APLICACIÓN DE PASARELA
⑮ APLICACIÓN DE PASARELA PASA DATOS DE PAGO Y RESPUESTA DE SOLICITUD DE PAGO A GSL
⑯ GSL ENVÍA DATOS FALSOS Y RESPUESTA DE SOLICITUD DE PAGO A SSA

FIG. 3

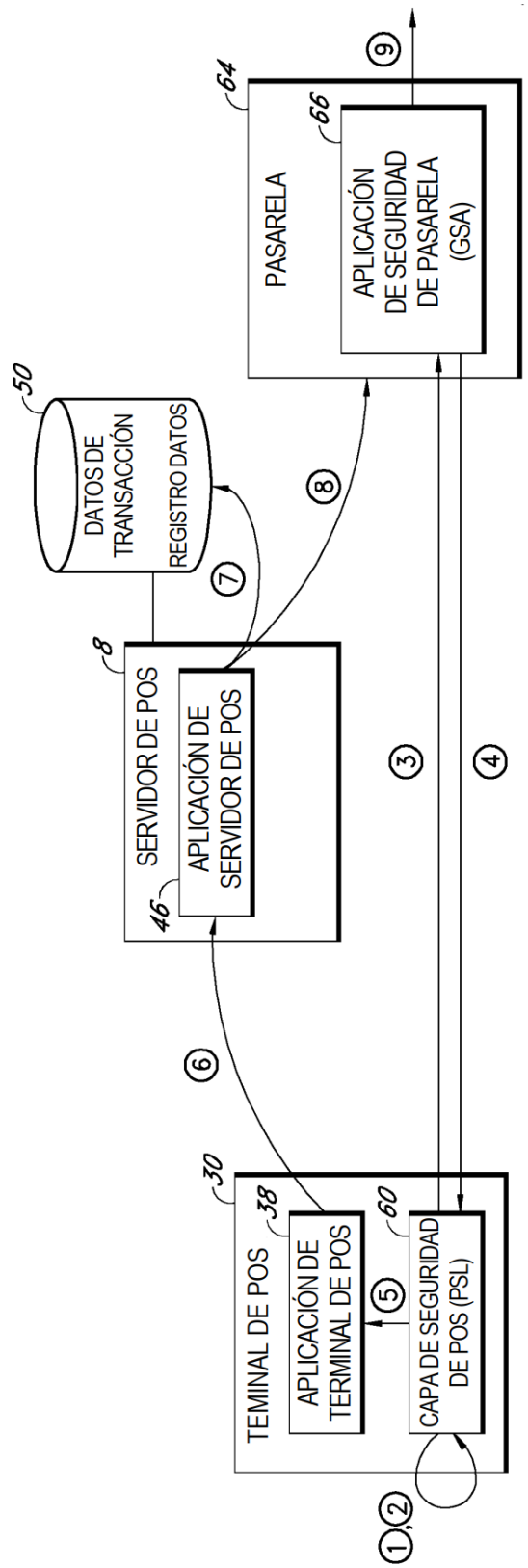


FIG. 4

① PSL INVOCADA DIRECTAMENTE POR ACCIÓN DE USUARIO, INDIRECTAMENTE POR ENTRADA DE DATOS DE TARJETA, O POR PROGRAMACIÓN
② PSL VISUALIZA INTERFAZ DE USUARIO DE PAGO Y CAPTURA INFORMACIÓN DE PAGO
③ PSL ENVÍA INFORMACIÓN DE PAGO CAPTURADA A GSA A TRAVÉS DE CANAL SEGURO
④ GSA DEVUELVE DATOS DE PAGO FALSOS
⑤ PSL PASA DATOS DE PAGO FALSOS A APLICACIÓN DE TERMINAL DE POS
⑥ APLICACIÓN DE TERMINAL DE POS PASA DATOS DE PAGO FALSOS A APLICACIÓN DE SERVIDOR DE POS
⑦ APLICACIÓN DE SERVIDOR DE POS REGISTRA TRANSACCIÓN CON DATOS DE PAGO FALSOS EN UNA BASE DE DATOS
⑧ APLICACIÓN DE SERVIDOR DE POS ENVÍA MENSAJE DE SOLICITUD DE PAGO A GSA
⑨ GSA TRANSMITE LOS DATOS DE PAGO REALES A UN PROCESADOR

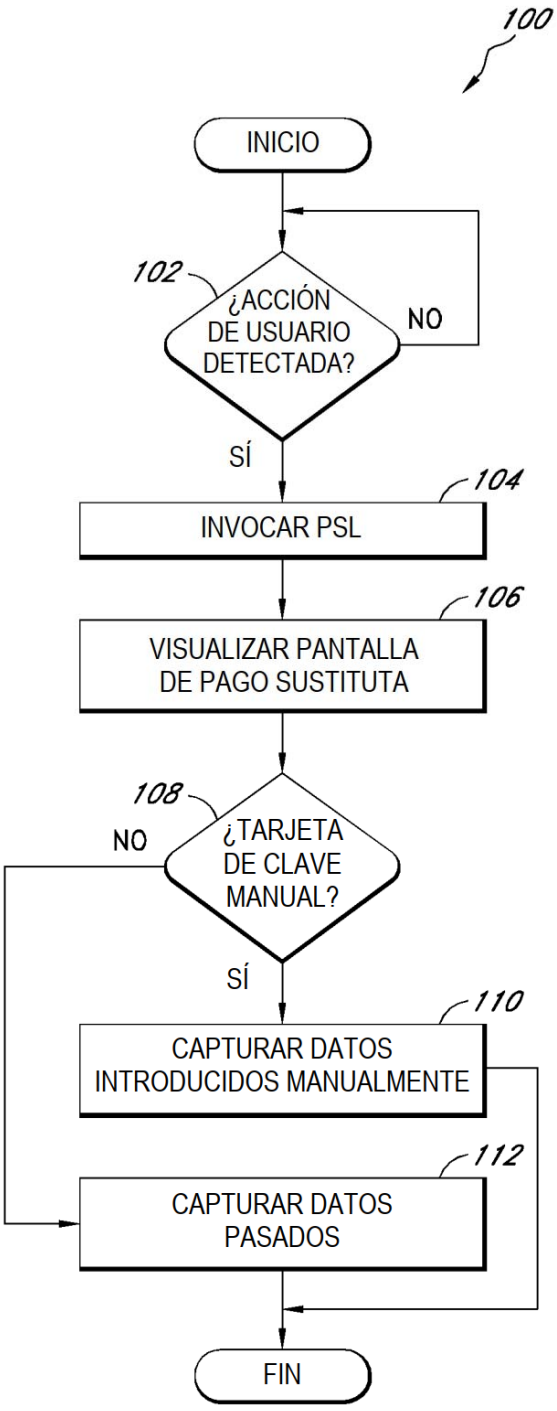

100
INICIO
102
¿ACCIÓN DE USUARIO DETECTADA?
NO
SÍ
104
INVOCAR PSL
106
VISUALIZAR PANTALLA DE PAGO SUSTITUTA
108
¿TARJETA DE CLAVE MANUAL?
NO
SÍ
110
CAPTURAR DATOS INTRODUCIDOS MANUALMENTE
112
CAPTURAR DATOS PASADOS
FIN

FIG. 5

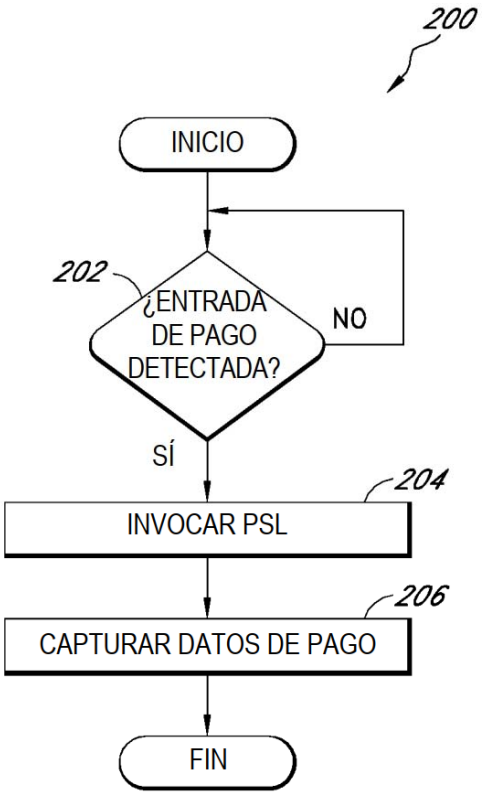

200
INICIO
202
¿ENTRADA DE PAGO DETECTADA?
NO
SÍ
204
INVOCAR PSL
206
CAPTURAR DATOS DE PAGO
FIN

FIG. 6

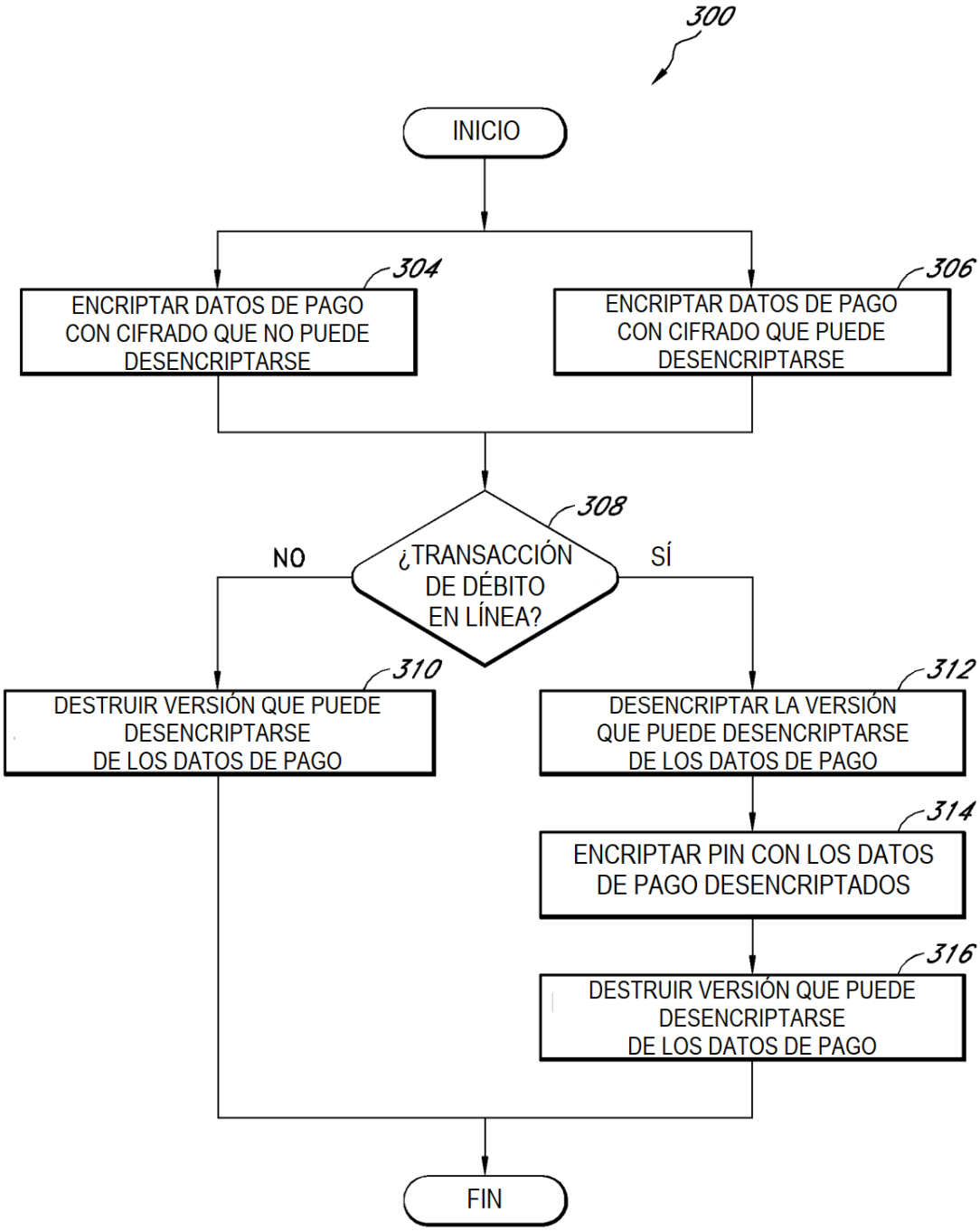

300
INICIO
304
ENCRIPTAR DATOS DE PAGO CON CIFRADO QUE NO PUEDE DESENCRIPTARSE
306
ENCRIPTAR DATOS DE PAGO CON CIFRADO QUE PUEDE DESENCRIPTARSE
308
¿TRANSACCIÓN DE DÉBITO EN LÍNEA?
NO
SÍ
310
DESTRUIR VERSIÓN QUE PUEDE DESENCRIPTARSE DE LOS DATOS DE PAGO
312
DESENCRIPTAR LA VERSIÓN QUE PUEDE DESENCRIPTARSE DE LOS DATOS DE PAGO
314
ENCRIPTAR PIN CON LOS DATOS DE PAGO DESENCRIPTADOS
316
DESTRUIR VERSIÓN QUE PUEDE DESENCRIPTARSE DE LOS DATOS DE PAGO
FIN

FIG. 7

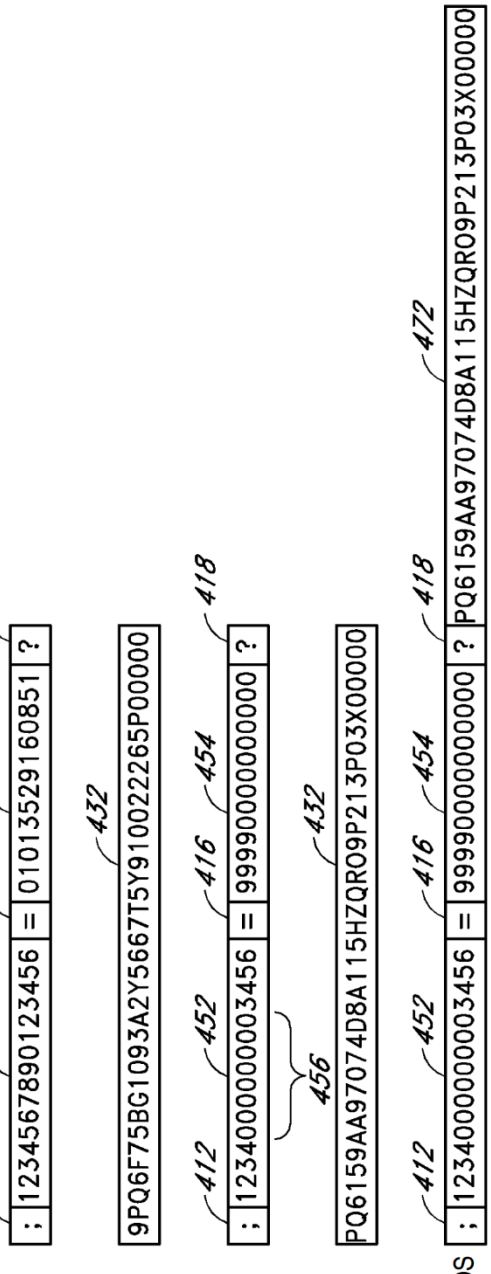

DATOS REALES
410
412
414
416
418
420
;
1234567890123456
=
0101352916085 1
?
DATOS ENCRIPTADOS
430
432
9PQ6F75BG1093A2Y5667T5Y910022265P00000
DATOS FALSOS
450
412
452
416
454
418
;
1234000000003456
=
9999000000000
?
456
DATOS RE-ENCRIPTADOS
460
432
PQ6159AA97074D8A115HZQRO9P213P03X00000
DATOS FALSOS
Y RE-ENCRIPTADOS COMBINADOS
470
412
452
416
454
418
472
;
1234000000003456
=
9999000000000
?
PQ6159AA97074D8A115HZQRO9P213P03X00000
DATOS REALES
410
412
414
416
418
420
;
1234567890123456
=
0101352916085 1
?

FIG. 8

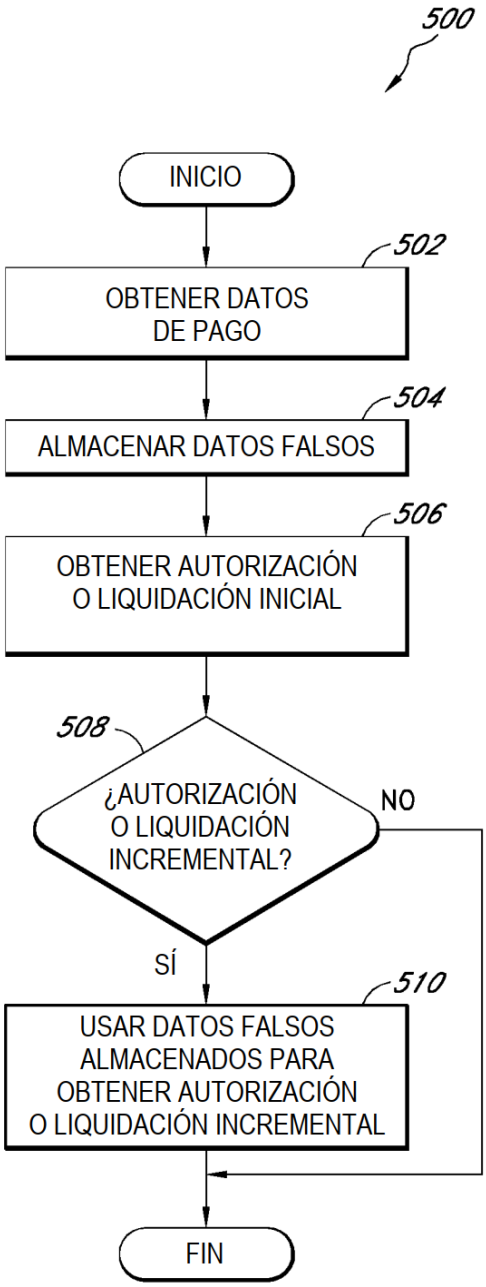

500
INICIO
502
OBTENER DATOS DE PAGO
504
ALMACENAR DATOS FALSOS
506
OBTENER AUTORIZACIÓN O LIQUIDACIÓN INICIAL
508
¿AUTORIZACIÓN O LIQUIDACIÓN INCREMENTAL?
NO
SÍ
510
USAR DATOS FALSOS ALMACENADOS PARA OBTENER AUTORIZACIÓN O LIQUIDACIÓN INCREMENTAL
FIN

FIG. 9