(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 633 344**

(51) Int. CI.:

G06F 21/55 (2013.01)
G06F 21/64 (2013.01)
G06F 21/77 (2013.01)
G06K 7/04 (2006.01)
G06Q 20/38 (2012.01)
G06Q 20/40 (2012.01)
G07F 7/10 (2006.01)
G07F 7/08 (2006.01)
G06F 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **14.11.2012 PCT/US2012/065017**

(87) Fecha y número de publicación internacional: **23.05.2013 WO13074631**

(96) Fecha de presentación y número de la solicitud europea: **14.11.2012 E 12805815 (3)**

(97) Fecha y número de publicación de la concesión europea: **12.04.2017 EP 2780854**

(54) Título: **Lector de tarjeta inteligente con una función de registro seguro**

(30) Prioridad:

14.11.2011 US 201161559503 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.09.2017

(73) Titular/es:

VASCO DATA SECURITY INTERNATIONAL GMBH (100.0%)
World-Wide Business Center Balz-Zimmermannstrasse 7
8152 Glattbrugg, CH

(72) Inventor/es:

BRAAMS, HARM

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Lector de tarjeta inteligente con una función de registro seguro

Campo técnico

La invención se refiere a asegurar la interacción remota de usuarios con servicios vía medios electrónicos a través del uso de firmas electrónicas. Más en particular, la invención se refiere a lectores de tarjetas inteligentes seguros para asegurar la firma de datos electrónicos por un usuario con una tarjeta inteligente.

Antecedentes de la invención

El creciente papel del acceso remoto e interacción de usuarios con todo tipo de servicios a través medios electrónicos ha dado lugar a una necesidad de que los usuarios sean capaces de realizar firmas electrónicas. Por razones de seguridad, dichas firmas electrónicas preferiblemente derivan de aplicar un algoritmo criptográfico parametrizado con una clave criptográfica que está asociada con el usuario por ciertos datos electrónicos. En algunos casos, el algoritmo criptográfico puede comprender una función de troceado (*hash function*) en clave mediante la cual una combinación de una clave secreta y los datos a firmar se envían a una función de troceado criptográfico unidireccional o una función de resumen (*digest function*) (tal y como, funciones de troceado criptográfico de las familias MD5, SHA-1, SHA-2 o SHA-256 de funciones de troceado) y los troceados o resúmenes resultantes constituyen la firma electrónica. En otros casos, el algoritmo criptográfico puede comprender un cifrado de bloque de encriptación o (desencriptación) simétrica, tal y como DES (norma de encriptación de datos) (triple) o AES (norma de encriptación avanzada) que se puede utilizar en modo CBC (concatenación de bloques) para generar un MAC (código de autenticación de mensaje) que puede constituir la firma electrónica. Incluso en otros casos, por ejemplo, en el contexto de una PKI (infraestructura de clave pública), la firma electrónica se puede generar utilizando un esquema de firma electrónica que está basado en criptografía asimétrica. En esos casos, los datos a firmar a menudo se trocean o envían a una función de resumen y el troceo o resumen resultante luego se encripta con un algoritmo de encriptación asimétrico utilizando la clave privada del usuario. Ejemplos de algoritmos criptográficos asimétricos utilizados para generar firmas electrónicas incluyen RSA (Rivest Shamir Adleman) y DSA (algoritmo de firma digital). Para mejorar la movilidad y seguridad, la clave secreta o privada a menudo se almacena en un contenedor seguro que, habitualmente, también es capaz de realizar operaciones criptográficas que involucran dicha clave. Una solución popular para generar firmas electrónicas comprende una tarjeta inteligente que comprende una memoria segura para almacenar de forma segura una o más claves secretas o privadas y otra información relacionada con la seguridad, tal y como PIN (número de identificación personal), perfiles de seguridad, contadores de intentos de PIN, ... , y un motor criptográfico para utilizar estas claves secretas o privadas con cierto algoritmo criptográfico simétrico o asimétrico para generar criptogramas de los datos recibidos de un ordenador anfitrión. La mayoría de las tarjetas inteligentes cumplen con al menos parte del conjunto de normas ISO/IEC 7816. En muchos casos, la funcionalidad criptográfica de la tarjeta inteligente está protegida por el requerimiento de que el usuario ingrese un PIN válido.

En un típico caso de uso, el usuario utiliza un dispositivo informático anfitrión, por ejemplo, un PC (ordenador personal) para interactuar con algún servicio remoto, por ejemplo, un sitio web de banca de Internet. El usuario tiene una tarjeta inteligente (tal y como se describe antes) que se inserta en un lector de tarjeta inteligente, que a su vez puede comunicarse con (es decir, puede recibir instrucciones de y devolver respuestas a) el dispositivo informático anfitrión. En un caso típico, el lector de tarjeta inteligente es más bien un dispositivo compacto que se acopla al dispositivo informático anfitrión mediante una conexión USB (bus serial universal). El usuario remoto revisa en el dispositivo informático anfitrión el documento o los datos a firmar. Una vez el usuario aprueba el documento o los datos a firmar, el documento o los datos se pueden enviar por la aplicación (que puede ser una aplicación dedicada o un navegador) a una biblioteca criptográfica para ser firmados. Ejemplos de API (interfaz de programación de aplicaciones) que a menudo se utilizan para la interfaz entre una aplicación y dicha biblioteca criptográfica incluyen MS-CAPI (Microsoft Cryptography API) y la API especificada por la norma PKCS#11 (Normas de Criptografía de Clave Pública # 11) publicada por los laboratorios RSA e incorporada en la presente memoria a modo de referencia. La biblioteca criptográfica (a menudo llamada "soporte intermedio") puede transformar la solicitud de la aplicación de una firma en una serie de instrucciones de comando-respuesta de la tarjeta inteligente que se intercambian con la tarjeta inteligente mediante un controlador de lector de tarjeta inteligente. Una API (interfaz de programación de aplicaciones) que a menudo se utiliza para dichos controladores de lector de tarjeta inteligente en ordenadores personales es PC/SC (ordenador personal/tarjeta inteligente). Previo que la tarjeta inteligente realice la firma real, al usuario generalmente se le solicita que ingrese un PIN en el dispositivo informático anfitrión, que luego se envía a la tarjeta inteligente para su verificación. En la mayoría de los casos, el lector de tarjeta inteligente es del tipo denominado "transparente", lo que significa que no realiza ninguna función de seguridad y que es, esencialmente, solo un medio de transporte para transmitir comandos desde el dispositivo informático anfitrión (de aquí en adelante también llamado "el ordenador anfitrión" o "el anfitrión") a la tarjeta inteligente y transmitir respuestas desde la tarjeta inteligente al ordenador anfitrión.

Descripción de la invención

Problema técnico

A pesar de que las tarjetas inteligentes criptográficas generalmente están equipadas con todo tipo de técnicas sofisticadas para frustrar todo tipo de ataques, hay un tema de seguridad fundamental en resultado, tal y como se describe antes, que no se puede resolver con medidas tomadas en la tarjeta inteligente. De hecho, un problema básico es que en el escenario que se plantea antes (que es típico para la forma en que se utilizan las tarjetas inteligentes para generar firmas electrónicas) todas las interacciones de usuario, incluyendo algunas operaciones muy sensibles, como el ingreso del PIN, se llevan a cabo en el ordenador anfitrión. En la gran mayoría de los casos, sin embargo, el ordenador anfitrión no se puede considerar una plataforma segura y fiable. De hecho, la mayoría de los dispositivos informáticos anfitriones son PCs o dispositivos similares que, debido a su propia naturaleza de ser plataformas informáticas abiertas para fines generales, son habitualmente muy vulnerables a todo tipo de virus y programas informáticos dañinos (malware). Esto hace que la configuración del escenario anterior sea muy vulnerable a ataques en los que un malware en el ordenador anfitrión del usuario interfiere con la interfaz de usuario del ordenador anfitrión, por ejemplo, para capturar el PIN que el usuario ingresa (por ejemplo, a través del uso de detectores de teclado) o incluso sustituyendo los datos a firmar que el usuario revisó y aprobó por datos fraudulentos antes de que los datos se envíen a la tarjeta inteligente para su firma.

Una solución es proveer lectores de tarjeta inteligente equipado con un teclado seguro (o algún otro tipo de interfaz de entrada del usuario segura para aceptar la entrada del usuario) que permita que el usuario ingrese el PIN de la tarjeta en el lector en vez de en un anfitrión inseguro, después de lo cual el lector luego puede enviar el PIN ingresado directamente a la tarjeta sin pasar por el anfitrión. Sin embargo, esta solución no ofrece protección contra ataques que interfieren con los datos a firmar, por lo cual los datos que se envían de forma efectiva a la tarjeta inteligente para su firma son diferentes a los datos que el usuario ha revisado y aprobado en el anfitrión.

Para resolver ese problema los lectores de tarjeta inteligente pueden estar equipados con un visualizador seguro (u otro tipo de interfaz de salida del usuario segura para presentar información al usuario) para presentar los datos a firmar al usuario para su aprobación, antes de enviar los datos a la tarjeta. Como tal, esta solución puede, sin embargo, ser más bien fácil de burlar. De hecho, basta con un malware en el ordenador anfitrión que invite al usuario a aprobar los datos en el ordenador anfitrión y a ingresar el PIN de la tarjeta, después de lo cual el malware puede sustituir los datos aprobados con datos fraudulentos y enviar los datos fraudulentos directamente a la tarjeta (utilizando el lector como un lector transparente) sin utilizar la característica de aprobación de datos segura del lector. Al usuario se lo puede convencer de aceptar esto mediante algún tipo de ingeniería social, por ejemplo, el malware puede aducir que hay algún tipo de problema técnico con el lector que evita la revisión de datos en el visualizador seguro del lector.

Para evitar este último tipo de ataque, el lector podría proveer algún tipo de cortafuegos, es decir, el lector puede escanear cada comando entrante de la tarjeta inteligente y verificar si corresponde a un comando de firma. En caso de que el comando recibido es un comando de tarjeta de firma entonces, se puede llevar a cabo una acción apropiada para garantizar que el anfitrión no es capaz de enviar comandos de firma a la tarjeta que contengan datos que no hayan sido presentados a (y aprobados por) el usuario en el visualizador seguro del lector. Por ejemplo, el lector puede automáticamente bloquear el comando (por ejemplo, cuando el lector admite un comando de lectura de firma seguro en el que el anfitrión envía datos a firmar al lector a partir de lo cual el lector presentará los datos al usuario en su visualizador seguro y, después de la aprobación del usuario, construirá y enviará a la tarjeta un comando de firma que contenga los datos aprobados). De manera alternativa, el lector puede extraer los datos a firmar del comando recibido, presentar esos datos al usuario, y sólo después de la aprobación del usuario, permitir que el comando de firma pase a la tarjeta.

Tal lector de tarjeta inteligente seguro que admite el ingreso de PIN seguro en el teclado del lector, una revisión y aprobación segura de datos de firma en el visualizador del lector, y un cortafuegos, hace todo lo posible para evitar ataques. Sin embargo, algunos problemas persisten. En particular, persisten los siguientes dos problemas:

En primer lugar, el cortafuegos del lector se sintoniza con el comando de firma como admitido por una tarjeta inteligente en particular. En la práctica, el conjunto de comandos de tarjetas inteligentes para firmar datos no está estandarizado. Como consecuencia, el mismo lector puede proteger muy bien un primer tipo de tarjetas inteligentes, pero puede dejar sin protección un segundo tipo de tarjetas inteligentes (admitiendo un comando de firma que el cortafuegos del lector no reconoce). Si el usuario cambia el tipo de tarjeta inteligente de firma o prefiere utilizar distintos tipos de tarjetas inteligentes, esto podría implicar problemas de seguridad. Este problema se puede resolver haciendo que el cortafuegos sea reconfigurable, sin embargo, con el fin de no introducir debilidades de seguridad, la reconfiguración del cortafuegos debe llevarse a cabo según un procedimiento seguro que puede significar una carga pesada para el lector y/o reducir la conveniencia de uso del lector.

La solicitud de patente europea EP 1 349 031 A1 describe un lector de tarjeta inteligente que cumple con los requisitos de FINREAD y presenta un visualizador para visualizar datos previo a su envío a la tarjeta inteligente y medios para garantizar que esta visualización solo pueda funcionar desde el programa de lector interno y no desde un programa que se ejecuta en el cliente. En un modo seguro, este lector verifica todos los comandos recibidos y decide si los envía hacia la tarjeta inteligente. Se monitoriza la aparición de condiciones de error.

Otro problema es que esta solución no evita que un atacante convenza a usuarios para que utilicen su tarjeta inteligente de firma en lectores de tarjeta inteligente inseguros o manipulados.

Por lo tanto, lo que se necesita es un lector de tarjeta inteligente seguro que sea capaz de admitir tarjetas inteligentes de muchos diferentes tipos de forma segura y que además ofrezca una manera de frustrar un ataque en el que un atacante convence al usuario de utilizar su tarjeta inteligente en un lector inseguro.

Solución técnica

La presente invención está definida por las reivindicaciones independientes 1 y 9. Las reivindicaciones dependientes 2-8 y 10-16 definen realizaciones adicionales.

A continuación se presenta un resumen simplificado de la presente invención con el fin de ofrecer una comprensión básica de algunos aspectos descritos en la presente memoria. Este resumen no es una visión general exhaustiva de la materia reivindicada. No se intenta identificar elementos clave o críticos de la materia reivindicada ni definir el alcance de la invención. Su único objeto es presentar algunos conceptos de la materia reivindicada de una forma simplificada, como un preludio a la descripción más detallada que se presentará a continuación.

La presente invención está basada en la comprensión de el/los inventor/es de que, a pesar de que puede ser muy difícil o incluso imposible garantizar que un atacante no será capaz de convencer a un usuario para que utilice un lector de tarjeta inseguro en vez de un lector de tarjeta seguro, para frustrar un ataque de ese tipo basta con detectar que se ha utilizado un lector de tarjeta inseguro.

En una realización según la invención, un método para detectar que se ha utilizado un lector de tarjeta inteligente inseguro comprende permitir al usuario utilizar un lector de tarjeta seguro que ofrezca pruebas de que se ha utilizado y suponer (o concluir), ante la falta de dichas pruebas que, en cambio, se ha utilizado un lector de tarjeta inteligente inseguro.

Otra realización según la invención comprende un lector de tarjeta inteligente seguro que está adaptado para probar que se ha utilizado el mismo para presentar, de forma segura, datos a firmar por el usuario, obtener la aprobación del usuario para esta operación de firma, y conseguir una firma de una tarjeta de los datos aprobados, al generar por sí mismo una firma de lector en datos representativos de eventos o acciones relacionados con la seguridad. En una realización, el lector está adaptado para ofrecer una firma electrónica de una representación de los datos que presenta al usuario para su aprobación y que envía a la tarjeta para su firma. En algunas realizaciones, el lector puede devolver tal firma de lector generada por el lector a la aplicación junto con la firma de tarjeta solicitada de los datos a firmar.

La invención además está basada en la comprensión de el/los inventor/es de que puede no ser necesario que el lector tenga un conocimiento preciso de los comandos de tarjeta inteligente sensibles si el ordenador anfitrión puede enviar dicha información al lector y si el lector es capaz de ofrecer pruebas de que las acciones que se llevan a cabo en el lector seguro (por ejemplo, qué datos se presentaron para la aprobación del usuario) y de qué comandos se intercambiaron con la tarjeta (por ejemplo, qué comando de firma se utilizó y con qué carga útil). Esto podría permitir la detección de cualquier discrepancia entre lo que realmente sucedió y lo que supone ha sucedido. Esto a su vez significa que la necesidad de un cortafuegos puede ser menor o que el cortafuegos puede ser menos restrictivo para que el lector pueda ser más flexible respecto a los tipos de tarjetas que se utilizan y los modos de uso de dichas tarjetas.

En algunas realizaciones según la invención, el lector de tarjeta inteligente seguro está adaptado para proveer una firma electrónica de una combinación de una representación de los datos que presenta al usuario para su aprobación y que envía a la tarjeta para su firma, y una representación de los datos que es indicativa de cómo se ha utilizado el lector seguro, p. ej., qué comandos ha recibido del ordenador anfitrión y/o qué interacciones de usuario han tenido lugar y/o qué parámetros de ajuste o configuración ha aplicado el lector cuando realizaba las operaciones solicitadas en los comandos recibidos del anfitrión y/o las interacciones de usuario que tuvieron lugar y/o qué comandos ha intercambiado el lector con la tarjeta inteligente.

En algunas realizaciones, el lector de tarjeta inteligente está adaptado para mantener uno o más registros para registrar datos representativos de comandos que el lector intercambia con el anfitrión y/o interacciones con el usuario y/o comandos intercambiados con la tarjeta inteligente. En algunas realizaciones, el lector puede estar adaptado para realizar una firma de datos que comprenden una representación de los contenidos de uno o más de estos registros. En algunas realizaciones, los parámetros de configuración o ajustes que se han aplicado, p. ej. al interactuar con el usuario o cuando se intercambian comandos con la tarjeta inteligente, también pueden estar comprendidos en los datos que firma el lector.

En algunas realizaciones, el lector puede comenzar el registro cuando entra en un modo seguro específico. En algunas realizaciones, el lector puede entrar a dicho modo seguro específico en respuesta a determinados comandos de lector que el lector recibe del anfitrión. En algunas realizaciones, el lector puede entrar a dicho modo seguro específico en respuesta a un evento relacionado con la tarjeta, tal y como una inserción de tarjeta. En algunas realizaciones, el lector puede reestablecer automáticamente uno o más de los registros que mantiene cuando entra en uno o más de los modos seguros que admite. En algunas realizaciones, el lector puede reestablecer automáticamente uno o más de los registros que mantiene en respuesta a un evento relacionado con la

tarjeta, tal y como un ingreso de tarjeta o retirada de tarjeta. En algunas realizaciones, el lector puede registrar cualquier comando de tarjeta inteligente que intercambia con la tarjeta inteligente mientras se encuentra en un modo seguro. En algunas realizaciones, el lector puede registrar cualquier comando de lector que el lector intercambia con el anfitrión mientras se encuentra en un modo seguro. En algunas realizaciones, el lector puede registrar datos que presenta al usuario para su aprobación. En algunas realizaciones, el lector puede registrar si el usuario aprobó datos que el lector le presentó. En algunas realizaciones, el lector puede registrar si se utilizó una función de ingreso de PIN segura para ingresar y verificar un PIN de tarjeta inteligente de un usuario.

En algunas realizaciones, el lector de tarjeta inteligente seguro puede mantener una copia de los datos agregados a uno o más de sus registros y, cuando se agregan datos a un registro, el lector puede concatenar los nuevos datos a los datos ya registrados. En algunas realizaciones, el lector de tarjeta inteligente seguro puede asociar a uno o más registros uno o más valores de troceo sobre los datos agregados a estos registros y, cuando se agregan datos a dicho registro, el lector puede actualizar el valor de troceo asociado con los datos que se están agregando.

En algunas realizaciones, el lector de tarjeta inteligente seguro admite la posibilidad de agregar contenidos de un registro a los contenidos de otro registro. En algunas realizaciones, el lector de tarjeta inteligente seguro está adaptado para enviar los contenidos de un registro a la tarjeta como un comando de tarjeta inteligente. En algunas realizaciones, el lector de tarjeta inteligente seguro está adaptado para enviar los contenidos de un registro a la tarjeta como parte de un comando de tarjeta inteligente. En algunas realizaciones, el lector de tarjeta inteligente seguro está adaptado para generar una firma de lector sobre los contenidos o parte de los contenidos de uno o más de los registros.

En algunas realizaciones, el lector de tarjeta inteligente seguro comprende una memoria segura para almacenar una o más claves de lector secretas o privadas que el lector utiliza con un algoritmo criptográfico para generar una firma de lector. En algunas realizaciones, los algoritmos criptográficos que el lector de tarjeta inteligente seguro utiliza para generar una firma de lector comprenden al menos uno de un algoritmo de encriptación o desencriptación simétrico, tal y como DES o AES, un algoritmo de troceado en clave criptográfico (por ejemplo, basado en SHA-1 o SHA-256), una función de resumen criptográfica (por ejemplo, basada en SHA-1 o SHA-256), o un algoritmo de firma digital basado en criptografía asimétrica (por ejemplo, basado en el algoritmo RSA o el algoritmo DSA o curvas elípticas).

Un aspecto de la invención provee un lector de tarjeta inteligente para generar firmas electrónicas en conjunción con una tarjeta inteligente insertada que comprende una interfaz de comunicación para comunicarse con un ordenador anfitrión; un conector de tarjeta inteligente para comunicarse con la tarjeta inteligente; un primer componente de memoria para almacenar de forma segura una o más claves criptográficas; un segundo componente de memoria para almacenar un registro; una interfaz de usuario que comprende una interfaz de salida del usuario para presentar información al usuario y una interfaz de entrada del usuario para recibir indicaciones de usuario; un componente de procesamiento de datos para comunicarse con el ordenador anfitrión, para comunicarse con la tarjeta inteligente y para controlar la interfaz de usuario; dicho lector de tarjeta inteligente adaptado para intercambiar comandos de tarjeta inteligente con una tarjeta inteligente utilizando el conector de tarjeta inteligente; dicho lector de tarjeta inteligente adaptado además para funcionar en un modo de registro seguro en el que el lector de tarjeta inteligente registra en dicho registro eventos relacionados con la seguridad respecto del lector o del uso del lector; y dicho lector de tarjeta inteligente adaptado además para generar una firma de lector en dicho registro utilizando al menos una de una o más de las claves criptográficas almacenadas en dicha primera memoria.

En un conjunto de realizaciones, el lector de tarjeta inteligente está además adaptado para llevar a cabo comandos de lector recibidos del ordenador anfitrión y para registrar en dicho registro al menos algunos de los comandos de lector recibidos. En algunas realizaciones, el lector de tarjeta inteligente está además adaptado para admitir uno o más comandos de lector que instruyan al lector para que presente datos a un usuario para revisión y aprobación por parte del usuario, para presentar al usuario los datos para revisión y aprobación utilizando la interfaz de salida, para capturar la aprobación o rechazo del usuario de los datos para revisión o aprobación utilizando la interfaz de entrada, y para registrar en dicho registro los datos para revisión y aprobación.

En otro conjunto de realizaciones, el lector de tarjeta inteligente además está adaptado para registrar en dicho registro al menos algunos comandos de tarjeta inteligente transparente intercambiados entre el anfitrión y la tarjeta inteligente. En algunas realizaciones, los comandos de tarjeta inteligente transparente que el lector registra comprenden comandos de tarjeta inteligente transparente para enviar a la tarjeta inteligente insertada los datos a firmar por la tarjeta inteligente. En otras realizaciones, los comandos de tarjeta inteligente transparente que el lector registra comprenden comandos de tarjeta inteligente transparente para obtener de la tarjeta inteligente insertada una firma de tarjeta electrónica generada sobre datos enviados. En incluso otras realizaciones, el lector está adaptado para registrar todos los comandos de tarjeta inteligente transparente en un período que va desde un primer punto en el tiempo a un segundo punto en el tiempo. En algunas de estas realizaciones, el período en el que el lector registra todos los comandos de tarjeta inteligente transparente comprende el período en el que los datos a firmar se envían a la tarjeta inteligente insertada o el período en el que la firma de tarjeta electrónica generada sobre los datos enviados se obtiene de la tarjeta inteligente insertada.

En incluso otro conjunto de realizaciones, el lector de tarjeta inteligente almacena un conjunto de datos de configuración que determinan al menos en parte qué eventos registra el lector. En algunas realizaciones, el lector de

tarjeta inteligente está adaptado para registrar el conjunto de datos de configuración actual. En algunas de estas realizaciones, el lector admite uno o más comandos de lector para cambiar el conjunto de datos de configuración.

En incluso otro conjunto de realizaciones, el lector de tarjeta inteligente además comprende un reloj y está adaptado para agregar uno o más sellos de tiempo al registro. En algunas realizaciones, el lector de tarjeta inteligente está adaptado para agregar un sello de tiempo a al menos algunos de los eventos registrados.

En otro conjunto de realizaciones, el lector de tarjeta inteligente además está adaptado para recibir una puesta a prueba a través de un comando de lector y registrar la puesta a prueba recibida.

En otro conjunto de realizaciones, el lector de tarjeta inteligente además comprende un contador y está adaptado además para registrar un valor relacionado con dicho contador. En algunas de estas realizaciones, el lector de tarjeta inteligente además está adaptado para aumentar automáticamente el valor de contador cuando entra en el modo de registro seguro o cuando genera la firma de lector en el registro.

En otro conjunto de realizaciones, el registro comprende múltiples ficheros de registro y la firma de lector en el registro comprende múltiples firmas sobre los múltiples ficheros de registro.

En otro conjunto de realizaciones, el lector de tarjeta inteligente además está adaptado para admitir un comando de lector para verificar la identidad del usuario. En algunas de estas realizaciones, el lector de tarjeta inteligente además está adaptado para registrar el resultado de la verificación de la identidad del usuario. En algunas de estas otras realizaciones, el lector de tarjeta inteligente además está adaptado para solicitar al usuario en la interfaz de salida del usuario que ingrese un valor de PIN y capturar en la interfaz de entrada del usuario un valor de PIN que el usuario ingresó y enviar el valor de PIN capturado a la tarjeta inteligente insertada para su verificación.

Otro aspecto de la invención provee un método para generar una firma electrónica sobre datos a firmar que comprende las etapas de conectar un lector de tarjeta inteligente a un ordenador anfitrión; insertar una tarjeta inteligente en el lector; hacer que el lector entre en un modo de registro seguro; enviar al lector datos para revisión y aprobación por parte del usuario; presentar al usuario, a través del lector que utiliza una interfaz de salida del usuario en el lector, los datos para revisión y aprobación por parte de un usuario; capturar, a través del lector que utiliza una interfaz de entrada del usuario en el lector, la aprobación del usuario de los datos presentados; registrar, a través del lector en un registro en el lector, los datos para revisión y aprobación; enviar a la tarjeta inteligente insertada datos a firmar, generando a continuación, a través de la tarjeta inteligente insertada, una firma de tarjeta electrónica sobre los datos a firmar enviados, y obteniendo a continuación de la tarjeta inteligente insertada la firma de tarjeta electrónica generada sobre los datos enviados; generar, a través del lector, una firma de lector electrónica sobre el registro en el lector que utiliza un algoritmo de firma de datos criptográfico parametrizado con una clave criptográfica almacenada en el lector y, a continuación, obtener la firma de lector electrónica sobre el registro generado por el lector. En algunas realizaciones, el método además comprende la etapa de registrar a través del lector en el registro sobre el lector los datos a firmar enviados a la tarjeta o la firma de tarjeta electrónica generada por la tarjeta inteligente insertada.

En un conjunto de realizaciones, el método además también comprende enviar a la tarjeta inteligente insertada datos a firmar y obtener de la tarjeta inteligente insertada la firma de tarjeta electrónica generada sobre los datos enviados, comprende que el ordenador anfitrión intercambie comandos de tarjeta inteligente transparente con la tarjeta inteligente insertada que utiliza el lector de tarjeta inteligente; y en donde registrar a través del lector en el registro sobre el lector los datos a firmar enviados a la tarjeta o la firma de tarjeta electrónica generada por la tarjeta inteligente insertada comprende registrar a través del lector en el registro sobre el lector al menos algunos de los comandos de tarjeta inteligente transparente intercambiados. En alguna de estas realizaciones, los comandos de tarjeta inteligente transparente que el ordenador anfitrión intercambia con la tarjeta inteligente insertada que utiliza el lector de tarjeta inteligente comprende al menos comandos de tarjeta inteligente transparente para enviar a la tarjeta inteligente insertada datos a firmar; y al menos algunos de los comandos de tarjeta inteligente transparente intercambiados que el lector registra en el registro sobre el lector comprenden al menos comandos de tarjeta inteligente transparente para enviar a la tarjeta inteligente insertada datos a firmar o comandos de tarjeta inteligente transparente para obtener de la tarjeta inteligente insertada una firma de tarjeta electrónica generada sobre datos enviados. En algunas de estas otras realizaciones, al menos alguno de los comandos de tarjeta inteligente transparente intercambiados que el lector registra en el registro sobre el lector comprenden todos los comandos de tarjeta inteligente transparente intercambiados durante un período determinado. En algunas de estas otras realizaciones, el período en el que el lector registra todos los comandos de tarjeta inteligente transparente intercambiados comprende el período en el que los datos a firmar se envían a la tarjeta inteligente insertada o el período en el que la firma de tarjeta electrónica generada sobre los datos enviados se obtiene de la tarjeta inteligente insertada.

En otro conjunto de realizaciones, el método además comprende configurar un conjunto de datos de configuración sobre el lector que determina al menos parcialmente qué eventos registra el lector en el registro sobre el lector. Algunas de estas realizaciones además comprenden la etapa de registrar, a través del lector, en el registro sobre el lector, el conjunto de datos de configuración actual. Alguna de estas realizaciones además comprende configurar el conjunto de datos de configuración de manera que el lector registre en un registro sobre el lector los datos para

revisión y aprobación. Otras de estas realizaciones además comprenden configurar el conjunto de datos de configuración de manera que el lector registre en un registro sobre el lector los datos a firmar enviados a la tarjeta o la firma de tarjeta electrónica generada por la tarjeta inteligente insertada. Incluso otras realizaciones además comprenden configurar el conjunto de datos de configuración de manera que el lector registre en un registro sobre el lector los comandos de lector para enviar datos al usuario para su revisión y aprobación. Incluso otras realizaciones además comprenden configurar el conjunto de datos de configuración de manera que el lector registre en un registro sobre el lector un conjunto de comandos de tarjeta inteligente transparente. Algunas de estas realizaciones además comprenden configurar el conjunto de datos de configuración de manera que el lector registre en un registro sobre el lector un conjunto de comandos de tarjeta inteligente transparente que comprende comandos de tarjeta inteligente para enviar a la tarjeta inteligente insertada datos a firmar o para obtener de la tarjeta inteligente insertada una firma electrónica generada sobre datos enviados a la tarjeta inteligente.

Incluso otro aspecto de la invención ofrece un método para asegurar el acceso de un usuario a una aplicación que comprende las etapas de proveer una tarjeta inteligente para firmar datos a un usuario; ofrecer a un usuario un lector de tarjeta inteligente según cualquiera de las realizaciones descritas anteriormente; proveer la interacción de usuario con la aplicación desde un ordenador anfitrión al que el lector está conectado; recopilar datos de transacción; recopilar datos a revisar y aprobar que están relacionados con los datos de transacción recopilados; recopilar datos a firmar que están relacionados con los datos de transacción recopilados; garantizar que la tarjeta inteligente está insertada en el lector de tarjeta inteligente; garantizar que el lector entre en un modo de registro seguro; enviar al lector datos para revisión y aprobación por parte del usuario; presentar al usuario, a través del lector, utilizando una interfaz de salida del usuario en el lector, los datos para revisión y aprobación por parte de un usuario; capturar, a través del lector, utilizando una interfaz de entrada del usuario en el lector, la aprobación del usuario de los datos presentados; registrar, a través del lector, en un registro sobre el lector los datos para revisión y aprobación; enviar a la tarjeta inteligente insertada datos a firmar, generando a continuación, a través de la tarjeta inteligente insertada, una firma de tarjeta electrónica sobre los datos enviados a firmar, y obteniendo a continuación de la tarjeta inteligente insertada la firma de tarjeta electrónica generada sobre los datos enviados; registrar, a través del usuario, en el registro sobre el lector los datos a firmar enviados a la tarjeta o la firma de tarjeta electrónica generada por la tarjeta inteligente insertada; generar, a través del lector, una firma de lector electrónica sobre el registro del lector, utilizando un algoritmo de firma de datos criptográficos parametrizado con una clave criptográfica almacenada en el lector y obteniendo a continuación la firma de lector electrónica sobre el registro generado por el lector; verificar la firma de tarjeta electrónica obtenida; verificar la firma de lector obtenida sobre el registro generado por el lector; verificar la coherencia entre el registro firmado por el lector y los datos de transacción recopilados.

En algunas realizaciones de este método, enviar a la tarjeta inteligente insertada datos a firmar comprende intercambiar entre el ordenador anfitrión y la tarjeta inteligente insertada comandos de tarjeta inteligente transparente para enviar datos a firmar a la tarjeta inteligente; y en el que registrar a través del lector en el registro sobre el lector los datos a firmar enviados a la tarjeta o la firma de tarjeta electrónica generada por la tarjeta inteligente insertada comprende registrar comandos de tarjeta inteligente intercambiados entre el ordenador anfitrión y la tarjeta inteligente insertada para enviar datos a firmar a la tarjeta inteligente o para recuperar una firma de tarjeta inteligente generada por la tarjeta inteligente insertada sobre datos enviados a la tarjeta para su firma.

Efectos ventajosos

Una ventaja importante de la presente invención es que permite detectar un ataque en el que un atacante convence al usuario de que utilice su tarjeta de firma con un lector inseguro. Otra ventaja de la presente invención es que permite detectar incoherencias entre lo que se supone ha sucedido en el lector y/o con la tarjeta y lo que realmente ha sucedido, de manera que un cortafuegos aplicado por el lector puede hacerse más laxo, lo que a su vez significa que el lector se puede utilizar con una variedad de tarjetas más amplia o una variedad de casos de uso más amplia.

A un experto en la técnica le resultarán evidentes más ventajas de la presente invención.

Breve descripción de los dibujos

Las funcionalidades y ventajas anteriores y otras funcionalidades y ventajas serán evidentes a partir de la siguiente descripción más particular de diversas realizaciones de la invención, tal y como se ilustra en los dibujos que acompañan.

La siguiente descripción y los dibujos anexos describen en detalle algunos aspectos ilustrativos de la materia reivindicada. Estos aspectos son indicativos, sin embargo, de solo algunas de las diversas formas en que los principios de la invención se pueden utilizar y la materia reivindicada está concebida para incluir dichos aspectos y sus equivalentes. Otras ventajas y funcionalidades novedosas de la materia reivindicada se volverán evidentes a partir de la siguiente descripción detallada de los aspectos de la invención cuando se los considera en conjunto con los dibujos.

La descripción detallada incluida a continuación en conexión con los dibujos adjuntos está concebida como una descripción de algunas realizaciones de la invención y no está concebida para representar las únicas formas en que la presente invención se puede construir y/o utilizar. La descripción incluye las funciones y la secuencia de etapas

para construir y hacer funcionar la invención en conexión con las realizaciones ilustradas. Sin embargo, se ha de comprender que se pueden lograr las mismas funciones y secuencias o sus equivalentes mediante diferentes realizaciones que también están concebidas para estar incluidas dentro del alcance de la invención.

La materia reivindicada se describe en referencia con los dibujos, en donde se utilizan números de referencia iguales para referirse a elementos similares a lo largo de toda la memoria. En la siguiente descripción, a fines de su explicación, se incluyen numerosos detalles específicos para ofrecer una comprensión exhaustiva de la invención. Sin embargo, puede resultar evidente que la materia reivindicada se puede poner en práctica sin estos detalles específicos. En otras instancias, se muestran estructuras y dispositivos conocidos en forma de diagrama de bloques con el fin de facilitar la descripción de la invención.

La Figura 1 ilustra un lector de tarjeta inteligente seguro según una realización de la invención;

la Figura 2 ilustra un sistema para realizar transacciones seguras según un aspecto de la invención; y

las Figuras 3a y 3b ilustran un método según un aspecto de la invención para asegurar transacciones remotas.

Forma(s) de llevar a cabo la invención

La Figura 1 ilustra un lector (100) de tarjeta inteligente seguro según un aspecto de la invención que comprende una interfaz de comunicación (110) para comunicarse con un ordenador anfitrión (99), una ranura (120) de lector de tarjeta inteligente para aceptar una tarjeta inteligente (98), un conector (130) de tarjeta inteligente para comunicarse con la tarjeta inteligente (98); al menos un componente de memoria (140) para almacenar de forma segura una o más claves criptográficas y/o uno o más ficheros de registro, una interfaz de usuario que comprende una interfaz de salida del usuario (151) para presentar información al usuario y una interfaz de entrada del usuario (152) para recibir indicaciones del usuario, uno o más componentes de procesamiento (160) para comunicarse con el ordenador anfitrión (99), para comunicarse con la tarjeta inteligente (98) y para controlar la interfaz de usuario (151/152). El lector (100) de tarjeta inteligente además está adaptado para funcionar en un modo de registro seguro en el que el lector (100) de tarjeta inteligente mantiene un registro, los contenidos del cual están relacionados con la seguridad y pueden ser indicativos de al menos algunos eventos relacionados con la seguridad que conciernen al lector y/o al uso del lector y que suceden mientras el lector está en el modo de registro seguro y que podrían tener un impacto a nivel seguridad. Los eventos a los que se puede adaptar al lector para que registre en un fichero de registro de esta manera pueden comprender comandos de lector que el lector recibe de una aplicación (p. ej. una aplicación local en el anfitrión o una aplicación remota en un servidor en conexión con el ordenador anfitrión), tal y como, por ejemplo, comandos de lector para presentar datos a un usuario para revisión o aprobación o para configurar o cambiar determinados datos de configuración, comandos de tarjeta inteligente que el lector intercambia con la tarjeta inteligente insertada (y que el lector puede haber recibido de una aplicación), tal y como, por ejemplo, comandos de tarjeta inteligente para permitir que la tarjeta firme datos, interacciones de usuario, tal y como, que el usuario apruebe o rechace datos que el lector presenta al usuario, otros eventos que pueden estar relacionados con la seguridad, tal y como detecciones de condiciones que pueden indicar un intento de manipular el lector. El lector (100) de tarjeta inteligente además está adaptado para generar una firma de lector en dicho registro utilizando al menos una de una o más de las claves criptográficas almacenadas por al menos un componente de memoria (140). Para generar la firma de lector, el lector puede comprender un componente de procesamiento (162) que comprende un motor criptográfico capaz de realizar cálculos criptográficos utilizando al menos una de una o más de las claves criptográficas almacenadas por al menos un componente de memoria (140). En algunas realizaciones, el medio de procesamiento (160) puede comprender el componente de procesamiento (162). En algunas realizaciones, los componentes mencionados anteriormente pueden estar contenidos dentro de un alojamiento (170). En algunas realizaciones, el lector puede estar adaptado para generar una firma de lector sobre dicho fichero de registro al aplicar un algoritmo criptográfico asimétrico a los contenidos del fichero de registro (o una representación del mismo, tal y como un resumen o troceado criptográfico) parametrizado con una clave privada de un par de claves público-privadas almacenadas en al menos un componente de memoria (140) del lector.

En algunas realizaciones, la interfaz de comunicación (110) para comunicarse con un ordenador anfitrión (99) puede comprender una interfaz USB que puede comprender un conector USB que se puede utilizar para conectar el lector (100) con un cable USB (97) a un puerto USB del ordenador anfitrión (99). En algunas realizaciones, los medios de procesamiento (160) para comunicarse con el ordenador anfitrión (99) pueden estar adaptados para admitir un protocolo USB con el ordenador anfitrión (99). En algunas realizaciones, el cable USB (97) puede estar fijo al lector (100). En otras realizaciones, el cable USB (97) puede desmontarse del lector (100).

En algunas realizaciones, la tarjeta inteligente (98) cumple o es compatible con al menos parte de las especificaciones ISO/IEC 7816 para tarjetas inteligentes, y la ranura (120) de lector de tarjeta inteligente para aceptar una tarjeta inteligente (98), el conector (130) de tarjeta inteligente para comunicarse con la tarjeta inteligente (98), y los medios de procesamiento (160) para comunicarse con la tarjeta inteligente (98) están adaptados para procesar tarjetas inteligentes que cumplan o sean compatibles con al menos parte de las especificaciones ISO/IEC 7816 para tarjetas inteligentes y están adaptados para procesar protocolos según al menos parte de las especificaciones ISO/IEC 7816.

En algunas realizaciones, la tarjeta inteligente (98) puede admitir funciones criptográficas para firmar datos. En algunas realizaciones, la tarjeta inteligente puede admitir una función de firma de datos basada en criptografía simétrica. En algunas realizaciones, la tarjeta inteligente puede admitir una función de firma de datos basada en criptografía asimétrica. En algunas realizaciones, la tarjeta inteligente comprende una memoria segura para almacenar de forma segura una o más claves criptográficas simétricas o asimétricas. En algunas realizaciones, la tarjeta inteligente comprende un agente criptográfico seguro para realizar operaciones criptográficas, tal y como encriptación y desencriptación simétrica o asimétrica y operaciones de firma de datos basadas en criptografía simétrica o asimétrica. En algunas realizaciones, el agente criptográfico seguro de la tarjeta inteligente puede estar adaptado para utilizar una o más claves criptográficas almacenadas en la memoria segura de la tarjeta inteligente. En algunas realizaciones, algunas de las operaciones o funciones admitidas por la tarjeta inteligente pueden estar protegidas por o estar condicionadas al correcto ingreso de un valor de PIN.

En algunas realizaciones, el lector (100) de tarjeta inteligente puede comprender un reloj (180) para ofrecer un valor de tiempo. En algunas realizaciones, este reloj (180) puede comprender un reloj en tiempo real. En algunas realizaciones, el lector de tarjeta inteligente puede utilizar el valor de tiempo provisto por el reloj (180) para dejar un sello de tiempo en determinados datos o acciones o eventos. En algunas realizaciones, el valor de tiempo puede ser una indicación del tiempo real absoluto, es decir, el valor de tiempo del lector tiene una relación directa con el tiempo universal real. En algunas realizaciones, el valor de tiempo puede ser un valor que es relativo a determinados eventos específicos de lector, tal y como, por ejemplo, el momento de producción del lector. En algunas realizaciones, el valor de tiempo del lector puede ser, p. ej., el tiempo Unix (en algunas realizaciones dentro de determinados márgenes de precisión), el tiempo GMT (Tiempo Medio de Greenwich) o UMT (Tiempo Métrico Universal). En algunas realizaciones, el reloj en tiempo real puede indicar el tiempo actual dentro de determinados márgenes de precisión. En algunas realizaciones, el reloj (180) indica un valor de tiempo que está sincronizado (dentro de determinados márgenes de precisión) con el valor de un reloj de un servidor.

Evidencia de manipulación, detección de manipulación y resistencia a la manipulación.

En algunas realizaciones, el lector (100) de tarjeta inteligente seguro está adaptado para garantizar que se detecten y/o resistan los intentos de manipular el lector. En algunas realizaciones, el alojamiento (170) del lector (100) de tarjeta inteligente está adaptado para resistir la apertura del alojamiento (170) y/o para aumentar la probabilidad de que un usuario se dé cuenta de intentos de abrir el alojamiento (170) mediante la deformación del alojamiento (170) (evidencia de manipulación). En algunas realizaciones, las partes que en conjunto forman el alojamiento (170) pueden estar soldadas o pegadas para que los intentos de desmontar estas partes conlleven, típicamente, la deformación obvia del alojamiento (170). En algunas realizaciones, el lector (100) comprende un interruptor que detecta la apertura del alojamiento (170). En algunas realizaciones, el lector (100) está adaptado para llevar a cabo una acción apropiada al detectar un intento de manipulación. En algunas realizaciones, el lector (100) puede borrar determinados datos sensibles, tal y como, claves criptográficas, o el lector (100) puede (quizás de forma irreversible) entrar en un modo de error o dejar de funcionar al detectar un intento de manipulación del lector (100). En algunas realizaciones, el lector (100) puede establecer y almacenar información relacionada con una detección de un intento de manipulación (tal y como, la fecha y hora y/o tipo de intento de manipulación) e incluir esa información en cálculos de firma de lector posteriores.

En algunas realizaciones, el lector (100) puede comprender una fuente de energía autónoma, por ejemplo, para ser capaz de activarse o permanecer activo incluso cuando no esté conectado al ordenador anfitrión (99), p. ej., para garantizar la detección de un intento de manipulación, para permitir que el reloj (180) mantenga el tiempo real, o para suministrar energía a una memoria volátil (140). En algunas realizaciones, la fuente de energía puede comprender una batería. En algunas realizaciones, la batería se puede reemplazar.

El lector (100) puede tener una interfaz de salida del usuario segura (p. ej., un visualizador seguro) y una interfaz de entrada segura (p. ej., un teclado seguro). En algunas realizaciones, el lector tiene una interfaz de salida que es segura en términos de que está completamente controlada por el lector y que no se puede utilizar para presentar datos o información al usuario mediante un proceso externo al lector, a menos que el lector lo autorice y controle. En algunas realizaciones, el lector tiene una interfaz de entrada que es segura en términos de que está completamente controlada por el lector y que no se puede utilizar para obtener datos o información del usuario mediante un proceso externo al lector, a menos que el lector lo autorice y controle. En algunas realizaciones, la seguridad de las interfaces de entrada y salida del usuario seguras se mantiene a través del lector, al no permitir ningún cambio en su firmware o al ofrecer un mecanismo de actualización de firmware seguro que sólo permite cambios al firmware del lector mediante un protocolo seguro que garantice que el lector sólo acepte actualizaciones de firmware autorizadas de una fuente de confianza.

El lector (100) puede estar adaptado para garantizar la seguridad del firmware y/o admitir ampliaciones de firmware seguras.

Los componentes de procesamiento (160) pueden comprender uno o más componentes de procesamiento. Estos componentes de procesamiento pueden comprender microchips, circuitos integrados, microcontroladores, microprocesadores, FPGAs (disposición de puertos programables de campo), ASICs (circuitos integrados de aplicaciones específicas) y similares.

La memoria (140) puede estar adaptada para almacenar de forma segura claves criptográficas. La memoria (140) puede comprender uno o más componentes de memoria que comprenden RAM (posiblemente respaldada por una batería), ROM, EEPROM, memoria flash u otros tipos de componentes de memoria. En algunas realizaciones, la memoria (140) puede comprender uno o más módulos SAM (módulo de acceso seguro). En algunas realizaciones, la memoria (140) puede comprender una o más tarjetas SIM (módulo de identificación de abonado). En algunas realizaciones, la memoria (140) puede comprender una o más tarjetas inteligentes internas o chips de tarjeta inteligente. El lector (100) puede estar adaptado para proteger la confidencialidad de datos sensibles almacenados, tal y como, por ejemplo, datos secretos que pueden comprender claves criptográficas. Estas claves criptográficas secretas pueden comprender claves criptográficas simétricas a utilizar con algoritmos criptográficos simétricos y/o claves criptográficas asimétricas a utilizar con algoritmos criptográficos asimétricos, tal y como claves privadas de pares de claves público/privadas. El lector (100) puede estar adaptado para borrar algunas áreas de memoria al detectar intentos de manipular el lector. Determinados contenidos de la memoria (140) se pueden encriptar.

El lector (100) también puede estar adaptado para almacenar certificados y/o claves públicas asociados con claves privadas almacenadas en la memoria (140).

El lector (100) puede estar adaptado para admitir capacidades criptográficas, tal y como admitir cálculos para algoritmos criptográficos asimétricos y/o algoritmos criptográficos simétricos y/o funciones de troceado. El lector puede estar adaptado para generar firmas de lector sobre datos representativos de eventos y acciones relacionados con la seguridad que pueden comprender datos representativos de comandos de lector que el lector recibe de un anfitrión (99), comandos de tarjeta inteligente que el lector intercambia con una tarjeta inteligente insertada (98), datos que el lector presenta al usuario para aprobación (p. ej., mediante una interfaz de salida del usuario (151)), o parámetros de configuración que el lector aplica cuando procesa cualquiera de los anteriores. El lector (100) de tarjeta inteligente puede además estar adaptado para mantener registros de determinados eventos y acciones relacionados con la seguridad, que pueden comprender intercambiar comandos de lector con un anfitrión, intercambiar comandos de tarjeta inteligente con una tarjeta inteligente insertada, y/o interacciones con un usuario. El lector (100) de tarjeta inteligente seguro puede estar adaptado para generar una firma de lector sobre uno o más de estos registros.

El lector (100) puede generar una firma de lector al aplicar a los datos a firmar un algoritmo criptográfico parametrizado con una clave criptográfica almacenada en memoria (140). El algoritmo criptográfico puede comprender una función de troceado en clave mediante la cual una combinación de una clave secreta y los datos a firmar se envían a una función de troceado criptográfico unidireccional o una función de resumen (tal y como, funciones de troceado criptográfico de las familias MD5, SHA-1, SHA-2 o SHA-256 de funciones de troceado) y los troceados o resúmenes constituyen la firma electrónica. El algoritmo criptográfico puede comprender un cifrado de bloque de encriptación o desear (desencriptación) simétrica, tal y como DES (norma de encriptación de datos) (triple) o AES (norma de encriptación avanzada) que se puede utilizar (p. ej., en modo CBC (concatenación de bloques) o algún otro modo de concatenación de bloques) para generar un MAC (código de autenticación de mensaje) que puede constituir la firma electrónica. El lector puede generar la firma de lector utilizando un esquema de firma electrónica que está basado en criptografía asimétrica. En estos casos, los datos a firmar a menudo pueden trocearse o enviarse a una función de resumen y el troceo o resumen resultante luego se encripta con un algoritmo de encriptación asimétrico utilizando la clave privada del usuario. Ejemplos de algoritmos criptográficos asimétricos utilizados para generar firmas electrónicas incluyen RSA (Rivest Shamir Adleman) y DSA (Algoritmo de Firma Digital).

En algunas realizaciones, el lector de tarjeta inteligente seguro está adaptado para inicializarse y/o personalizarse con una o más claves de lector secretas o privadas durante o después de producción. En algunas realizaciones, el lector de tarjeta inteligente seguro admite un protocolo de intercambio de datos seguro para actualizar datos de lector sensibles, tal y como parámetros de configuración de seguridad y/o claves criptográficas. En algunas realizaciones, el lector de tarjeta inteligente seguro comprende un componente seguro capaz de generar claves criptográficas. En algunas realizaciones, el lector de tarjeta inteligente seguro puede comprender un componente seguro capaz de generar un par de claves público-privadas. En algunas realizaciones, el lector de tarjeta inteligente seguro puede comprender un componente seguro capaz de generar números aleatorios.

Cortafuegos.

El lector puede admitir un cortafuegos que examine comandos de tarjeta inteligente enviados por el anfitrión y concebidos para la tarjeta inteligente, según el cual el lector puede bloquear comandos dependiendo de ciertos criterios. En algunas realizaciones, el lector puede configurar el cortafuegos dependiendo del tipo de tarjeta. En algunas realizaciones, el lector determina el tipo de tarjeta mediante uno o más comandos de tarjeta inteligente de SELECCIONAR APLICACIÓN. En alguna realización, el cortafuegos mantiene una lista de comandos de tarjeta inteligente que se deben bloquear (y a otros comandos de tarjeta inteligente se les puede permitir el paso). En algunas realizaciones, el cortafuegos mantiene una lista de comandos de tarjeta inteligente que tienen permitido el paso (y todos los otros comandos de tarjeta inteligente pueden estar bloqueados). En algunas realizaciones, el cortafuegos reconoce los comandos de tarjeta inteligente en base al valor de ciertos bytes en la cabecera de comando (tal y como los bytes CLA, INS, P1 y/o P2). En algunas realizaciones, el lector puede tener un cortafuegos que puede investigar y/o cambiar los contenidos de algunos comandos de tarjeta inteligente. Los comandos de

tarjeta inteligente que el lector recibe del anfitrión y que el anfitrión concibe para ser reenviados por el lector a la tarjeta y que el lector reenvía a la tarjeta sin bloquearlos o alterar sus contenidos pueden denominarse "comandos de tarjeta inteligente transparente". Si el lector trabaja en un modo en que un cortafuegos no bloquea o altera los comandos de tarjeta inteligente, entonces puede decirse que el lector trabaja en un modo transparente.

Comandos de lector;

El lector puede estar adaptado para recibir y llevar a cabo comandos del ordenador anfitrión (es decir, por ejemplo una aplicación local en el ordenador anfitrión o una aplicación remota en un servidor de aplicaciones conectado al ordenador anfitrión). Dichos comandos de lector pueden comprender comandos para cambiar datos de configuración del lector, para permitir que el lector entre en un modo de registro seguro, para permitir que el usuario lleve a cabo una verificación de identidad del usuario segura (como un ingreso de PIN seguro), para permitir que el lector presente determinados datos al usuario, y para permitir que el usuario revise y apruebe o rechace los datos presentados, etc.

Autenticación de usuario segura.

En algunas realizaciones, el lector puede admitir comandos de lector que se pueden utilizar para instruir al lector para que autentique al usuario de forma segura.

Por ejemplo, en algunas realizaciones, el lector puede admitir comandos de lector que se pueden utilizar para instruir al lector para que solicite al usuario para que ingrese un PIN (o contraseña), capture el PIN (o contraseña) ingresada por el usuario y envíe el PIN (o contraseña) capturado a la tarjeta inteligente para que la tarjeta inteligente lo verifique. En algunas realizaciones, dichos comandos de lector de ingreso de PIN seguro pueden contener parámetros que indican al lector cómo construir un comando de tarjeta inteligente de Verificar PIN. En algunas realizaciones, el lector está adaptado para borrar de la memoria todas las copias de un valor de PIN o contraseña después de que se ha enviado a la tarjeta inteligente para verificación.

En algunas realizaciones, el lector puede comprender algún tipo de dispositivo de captura biométrica, tal y como, por ejemplo, huellas digitales, y el lector puede admitir comandos de lector que se pueden utilizar para instruir al lector para que (opcionalmente) solicite al usuario que envíe sus datos biométricos al lector, capture los datos biométricos y verifique los datos biométricos capturados (por ejemplo, con el fin de autenticar al usuario). En algunas realizaciones, los datos biométricos pueden verificarse mediante el envío, por parte del lector, de los datos biométricos capturados hacia la tarjeta inteligente y la verificación, por parte de la tarjeta inteligente, de los datos biométricos capturados. En algunas realizaciones, los datos biométricos se pueden verificar, por parte del lector, al obtener de la tarjeta inteligente los datos biométricos de referencia y comparar los datos biométricos del usuario capturados con los datos biométricos de referencia obtenidos de la tarjeta inteligente. En algunas realizaciones, el lector está adaptado para borrar de la memoria todas las copias de datos biométricos después de que se han enviado a una tarjeta inteligente para verificación o después de que el lector los ha utilizado a los fines de autenticación de un usuario.

Firma segura.

El lector puede estar adaptado para ofrecer un modo de firma seguro en el que el anfitrión o una aplicación que interactúe con el lector envíe datos al lector para que la tarjeta los firme. En dicho modo de firma seguro, el lector presenta los datos a firmar al usuario y solicita al usuario que apruebe los datos. Después de que el usuario aprueba los datos, el lector envía el comando de firma (o una serie de comandos) a la tarjeta que contiene los datos a firmar (o una representación de los mismos, tal y como un troceado de los datos a firmar). El lector recibe la firma de la tarjeta y la devuelve al anfitrión. En algunas realizaciones, el lector puede admitir comandos de lector que permiten a una aplicación que interactúa con el lector enviar datos al lector para que la tarjeta los firme, mediante lo cual la aplicación puede indicar al lector cuáles de estos datos deben ser revisados y aprobados por el usuario y cuáles de estos datos no deben ser revisados y aprobados por el usuario antes de que los datos sean firmados por la tarjeta.

Revisión y aprobación de los datos.

En algunas realizaciones, el lector puede admitir comandos de lector que permiten que una aplicación que envía datos al lector sea revisada y aprobada por el usuario. En algunas realizaciones, dichos comandos de lector pueden incluir comandos de lector para iniciar una operación de firma segura, tal y como se describe antes. En algunas realizaciones, dichos comandos de lector pueden incluir comandos de lector que no instruyan al lector para que automáticamente permita a la tarjeta firmar los datos revisados y aprobados. Por ejemplo, en algunas realizaciones, el lector puede admitir comandos de lector que permitan a una aplicación enviar datos al lector para que los revise y apruebe el usuario, mediante lo cual el lector, después de la aprobación de los datos por parte del usuario, agrega los datos aprobados (o datos representativos de los datos aprobados, tal y como comando/s de lector que contiene/n estos datos o un troceado de estos datos) a un fichero de registro. A continuación, la aplicación puede enviar los mismos datos a la tarjeta para su firma, por ejemplo, enviando comandos de tarjeta inteligente transparente a la tarjeta. El lector puede también agregar esto al fichero de registro. A continuación, el lector puede firmar el fichero de

registro. La firma del lector en el fichero de registro prueba que los datos firmados por la tarjeta también han sido revisados y aprobados por el usuario en el lector seguro.

En algunas realizaciones, los datos a revisar y aprobar por el usuario son visualizados por el lector en, p. ej., el visualizador (seguro) del lector. En algunas realizaciones, los datos a revisar y aprobar por el usuario pueden presentarse al usuario a través del lector, p. ej., a través de generación de voz artificial. En algunas realizaciones, el usuario puede aprobar los datos, p. ej., al presionar un botón de ACEPTAR en el teclado del lector. En algunas realizaciones, el usuario puede rechazar los datos, p ej., al presionar un botón de cancelar en el teclado (seguro) del lector.

En algunas realizaciones, si los datos a revisar no cupieran en el visualizador del lector, el lector puede visualizar una parte de los datos y dar al usuario la posibilidad de desplazarse verticalmente por el resto de los datos, o el lector puede dividir los datos en una secuencia de bloques de datos que quepa cada una en el visualizador y darle al usuario la posibilidad de navegar por estos bloques de datos. En algunas realizaciones, el usuario sólo puede indicar la aprobación después de haberse desplazado verticalmente por todos los datos o después de haber navegado por todos los bloques de datos.

Modo de registro seguro.

El lector puede estar adaptado para proveer un modo de registro seguro en el que mantiene uno o más registros. El lector puede ofrecer comandos de lector para abrir dicho modo de registro seguro. El lector puede reestablecer los contenidos de uno o más de los registros al entrar en el modo de registro seguro. En algunas realizaciones, el lector puede admitir comandos de lectura que permitan al anfitrión reestablecer los registros. El lector puede agregar a uno de los registros datos indicativos de al menos parte de los comandos de lector que recibe mientras se encuentra en este modo. El lector puede admitir comandos de lector que permitan al anfitrión agregar datos a al menos uno de los registros. El lector puede admitir comandos de lector que permitan al anfitrión instruir al lector para que construya un comando de tarjeta inteligente utilizando los contenidos de un registro y envíe ese comando de tarjeta inteligente a la tarjeta inteligente. El lector puede admitir comandos de lector que permitan al anfitrión instruir al lector para que presente ciertos datos al usuario en la interfaz de salida del usuario del lector para la aprobación del usuario. El lector puede admitir comandos de lector que permitan al anfitrión instruir al lector para que presente contenidos de un registro al usuario para su aprobación. Una vez el usuario apruebe los datos, el lector puede automáticamente agregar los datos aprobados a uno de los registros. En algunas realizaciones, el lector puede admitir comandos de lector que permitan al anfitrión instruir al lector para que agregue contenidos de un registro a los contenidos de otro registro. El lector puede estar adaptado para agregar automáticamente a uno de los registros datos representativos de comandos de lector recibidos del anfitrión mientras se encontraba en el modo de registro seguro. El lector puede estar adaptado para agregar automáticamente a uno de los registros datos representativos de comandos de tarjeta inteligente y respuestas intercambiados entre el lector y la tarjeta inteligente mientras se encontraba en el modo de registro seguro. En algunas realizaciones, el lector puede estar adaptado para agregar automáticamente a uno de los registros datos representativos de algunos o todos los comandos de tarjeta inteligente y sus correspondientes respuestas intercambiados entre el lector y la tarjeta inteligente mientras se encontraba en el modo de registro seguro. Mientras se encuentra en el modo de registro seguro, el lector puede activar un cortafuegos. Este cortafuegos puede bloquear determinados o todos los comandos de tarjeta inteligente que el anfitrión solicite al lector que intercambie con la tarjeta inteligente.

Mecanismos que un lector puede utilizar cuando agrega datos a un fichero de registro.

En algunas realizaciones, cuando el lector registra nuevos datos, puede agregar esos nuevos datos a un fichero de registro, añadiendo los datos nuevos que se están registrando a los datos que ya se habían agregado al fichero de registro antes. En algunas realizaciones, el lector puede agregar nuevos datos a un fichero de registro al actualizar un valor de troceado o resumen que está asociado al fichero de registro. En algunas realizaciones, el lector puede, al agregar nuevos datos a un fichero de registro, tanto añadir los nuevos datos a los datos que ya se habían registrado antes como actualizar un valor de troceado o resumen que está asociado con el fichero de registro.

En algunas realizaciones, el lector puede formatear datos que agrega a un fichero de registro y agregar los datos formateados al fichero de registro, tal y como se indica antes. Por ejemplo, el lector puede agregar separadores para distinguir elementos de datos consecutivos que se están agregando al fichero de registro. En algunas realizaciones, el lector puede agregar delimitadores de comienzo y fin a los elementos de datos que se están agregando al fichero de registro. En algunas realizaciones, los elementos de datos que se están agregando al fichero de registro se pueden etiquetar antes de que se agreguen al fichero de registro. En algunas realizaciones, los elementos de datos que se están agregando a un fichero de registro están integrados a una estructura TLV (valor de longitud de etiqueta) antes de que se agreguen al fichero de registro. En algunas realizaciones, las etiquetas se pueden utilizar para indicar la naturaleza de los diversos elementos de datos que se están agregando a un fichero de registro. Por ejemplo, se pueden utilizar diferentes etiquetas para indicar si determinados datos representan un comando o respuesta de tarjeta, o un comando o respuesta de lector, o datos de configuración de lector, o datos relacionados con la interacción de usuario (p. ej., indicar si el lector presentó determinados datos para revisión, y si el usuario aprobó los datos presentados para revisión), o datos que representan determinados eventos (por ejemplo, la detección de los que podrían ser intentos de manipular el dispositivo), o si los datos representan un sello de tiempo.

En algunas realizaciones, los elementos de datos pueden tener un sello de tiempo antes de que se agreguen a un fichero de registro. En algunas realizaciones, un sello de tiempo puede ser una parte de una estructura de formateo que se aplica a los datos que se agregan a un fichero de registro.

En algunas realizaciones, el lector puede almacenar los contenidos de un fichero de registro en uno o más ficheros de un sistema de ficheros. En otras realizaciones, el lector puede almacenar los contenidos de un fichero de registro en otro tipo de estructura de datos que mantiene en algún componente de memoria.

El lector puede estar adaptado para admitir comandos de lectura que permiten al anfitrión instruir al lector para que genere una firma de lector sobre datos contenidos en uno o más de los registros. El lector también puede estar adaptado para generar automáticamente una firma de lector sobre uno de los registros cuando suceden ciertos eventos. Por ejemplo, el lector puede generar automáticamente una firma de lector cuando ha intercambiado un comando de tarjeta inteligente con la tarjeta inteligente que contiene datos aprobados por el usuario. O, puede generar automáticamente una firma de lector cuando ha intercambiado un comando de tarjeta inteligente con la tarjeta inteligente que el lector construyó a partir de contenidos de un registro. O, puede generar automáticamente una firma de lector sobre uno de los registros cuando abandona el modo de registro seguro.

En algunas realizaciones, el lector admite comandos de lector para recuperar los contenidos de un fichero de registro. En algunas realizaciones, el lector puede permitir la recuperación de los contenidos de algunos ficheros de registros, pero no de otros ficheros de registros. En algunas realizaciones, los contenidos de algunos ficheros de registro sólo se pueden recuperar una vez que el lector haya generado una firma sobre estos contenidos. En algunas realizaciones, los contenidos de los ficheros de registros no se pueden recuperar del lector. En algunas realizaciones, los contenidos de algunos ficheros de registro se pueden recuperar junto con una firma de lector sobre esos contenidos.

Configurabilidad del modo de registro seguro.

En algunas realizaciones, se pueden configurar determinados aspectos de la forma en que funciona el lector cuando está en un modo de registro seguro. Por ejemplo, se puede configurar qué datos o eventos debe registrar el lector y en qué registro debe registrarlos el lector. También se puede configurar en qué situaciones el lector debe generar una firma y sobre qué datos o fichero de registro. En algunas realizaciones, algunos de los parámetros de configuración del modo de registro seguro se pueden embeber en el código del lector y no se pueden cambiar. En algunas realizaciones, los parámetros de configuración embebidos en el código pueden estar implícitos, ya que están embebidos en la lógica del firmware del lector. En otras realizaciones, algunos parámetros de configuración pueden estar embebidos explícitamente en el código en forma de valores de parámetros embebidos en el código. En algunas realizaciones, algunos de los parámetros de configuración del modo de registro seguro pueden estar almacenados en la memoria no volátil del lector. En algunas realizaciones, algunos de los parámetros de configuración del modo de registro seguro que están almacenados en la memoria no volátil del lector pueden actualizarse, por ejemplo, utilizando comandos de lector de actualización de parámetros seguros. En algunas realizaciones, algunos de los parámetros de configuración del modo de registro seguro pueden ofrecerse al lector como parte de un comando de lector. En algunas realizaciones, algunos parámetros de configuración del modo de registro seguro que se proveen al lector como parte de un comando de lector pueden, al menos temporalmente, anular los parámetros de configuración del modo de registro seguro que están almacenados en una memoria no volátil o que están embebidos en el código. En algunas realizaciones, al menos algunos parámetros de configuración del modo de registro seguro que están embebidos en el código pueden ser anulados por parámetros de configuración del modo de registro seguro que están almacenados en la memoria no volátil del lector y que pueden actualizarse de forma segura, p. ej., utilizando comandos de actualización de parámetros de lector seguros. En algunas realizaciones, algunos de los parámetros de configuración del modo de registro seguro pueden ofrecerse al lector como parte de un comando de lector para entrar en un modo de registro seguro. En algunas realizaciones, si se proveen algunos parámetros de configuración del modo de registro seguro mediante un comando de lector, se pueden agregar automáticamente datos representativos de este comando a un fichero de registro. En algunas realizaciones, cuando un comando de lector instruye al lector para que entre en un modo de registro seguro, ese comando puede comprender un conjunto de parámetros de configuración del modo de registro seguro y datos representativos de al menos algunos de los parámetros de configuración del modo de registro seguro aplicables para este modo de registro seguro se registran automáticamente.

Sello de tiempo.

En algunas realizaciones, el lector (100) puede estar adaptado para dejar un sello de tiempo en determinados datos. El lector (100) puede utilizar el tiempo provisto por un reloj (180) para dejar el sello de tiempo en datos. Los datos en los que el lector puede dejar un sello de tiempo pueden incluir datos que se agregan a uno de los registros, datos que firma la tarjeta (98), datos firmados por el lector (100), firmas generadas por la tarjeta, o firmas generadas por el lector. En algunas realizaciones, a cada elemento de datos que se agrega a un fichero de registro se le deja automáticamente un sello de tiempo. En algunas realizaciones, solo a elementos específicos de datos que se agregan a un fichero de registro se les deja un sello de tiempo. En algunas realizaciones, el lector ofrece un sello de tiempo sobre eventos específicos, tal y como el momento en que el lector entra o abandona un modo de registro seguro o el momento en que se solicita u obtiene una firma de una tarjeta, o el momento en que sucede

determinadas interacciones de usuario, tal y como presentar datos al usuario para aprobación u obtener aprobación del usuario para los datos. En algunas realizaciones, el lector admite comandos de lector que permiten instruir al lector para que agregue un sello de tiempo a un fichero de registro. En algunas realizaciones, el lector puede estar adaptado para agregar un elemento de datos que representa el tiempo de lector actual a un fichero de registro, p. ej., en respuesta a un comando de lector específico o en respuesta a un evento específico.

Medidas antireproducción

En algunas realizaciones, el lector (100) puede estar adaptado para admitir determinadas medidas para frustrar determinados tipos de ataques de reproducción. Por ejemplo, en algunas realizaciones, el lector puede aplicar un sello de tiempo a una firma de lector o agregar un sello de tiempo a un fichero de registro o a datos que se agregan a un fichero de registro. En algunas realizaciones, el lector puede estar adaptado para generar números aleatorios y puede agregar un número aleatorio a los datos que firma el lector o puede agregar un número aleatorio a un fichero de registro. En algunas realizaciones, el lector puede mantener un contador que incrementa (o disminuye) de manera monótona cada vez que el lector utiliza su valor, o un equivalente del mismo, tal y como un valor que evoluciona de manera monótona, es decir, un valor que se reemplaza cada vez que una función del valor actual lo utiliza, p. ej., un troceado del valor actual. En algunas realizaciones, el lector puede agregar tal contador o valor que evoluciona de manera monótona a un fichero de registro o a los datos que firma. En algunas realizaciones, el lector puede estar adaptado para recibir de una aplicación externa a través de un comando de lector una puesta a prueba del servidor, tal y como un número impredecible (que puede comprender un número aleatorio o pseudoaleatorio) o un valor de tiempo o un valor de contador de servidor, y el lector puede agregar esta puesta a prueba del servidor a los datos que el lector firma o a los datos que el lector agrega al fichero de registro. En algunas realizaciones, dicha puesta a prueba del servidor puede ser parte de los datos en un comando de lector para instruir al lector para que entre en un modo de registro seguro. En algunas realizaciones, dicha puesta a prueba del servidor puede ser parte de los datos que la aplicación envía al lector para que la tarjeta los firme. En algunas realizaciones, dicha puesta a prueba del servidor puede ser parte de los datos que la aplicación envía al lector para que los revise y apruebe el usuario.

Comunicaciones seguras con la tarjeta inteligente.

En algunas realizaciones, el lector (100) está adaptado para asegurar sus comunicaciones con la tarjeta inteligente (98). Por ejemplo, en algunas realizaciones, el lector puede estar adaptado para autenticar la tarjeta inteligente, p. ej., verificando certificados de la tarjeta inteligente o verificando Códigos de Autenticación de Mensaje generados por la tarjeta inteligente. En algunas realizaciones, el lector puede ser capaz de autenticarse a sí mismo ante la tarjeta inteligente, p. ej., generando Códigos de Autenticación de Mensaje que pueden ser verificados por la tarjetas. En algunas realizaciones, el lector puede estar adaptado para generar claves de sesión simétricas que comparte con una tarjeta inteligente insertada. En algunas realizaciones, el lector está adaptado para encriptar y/o desencriptar comandos y/o respuestas que intercambia con la tarjeta inteligente. Por ejemplo, el lector puede estar adaptado para encriptar comandos de tarjeta inteligente en los que el lector envía datos sensibles a la tarjeta, tal y como, datos biométricos o un valor de PIN o contraseña. En algunas realizaciones, el lector puede estar adaptado para desencriptar datos encriptados que provienen de las tarjetas inteligentes, tal y como, por ejemplo, datos biométricos de referencia.

Comunicaciones seguras con una aplicación.

En algunas realizaciones, el lector (100) está adaptado para asegurar sus comunicaciones con una aplicación externa que se comunica con el lector a través de comandos de lector. La aplicación externa se puede ejecutar (completa o parcialmente) en un ordenador anfitrión al que está conectado el lector. La aplicación externa también se puede ejecutar (completa o parcialmente) en un servidor de aplicaciones remotas que está conectado mediante una red informática a un ordenador anfitrión al que está conectado el lector. En algunas realizaciones, el lector puede compartir una clave secreta con una aplicación externa que se puede utilizar para asegurar las comunicaciones entre el lector y la aplicación. En algunas realizaciones, el lector puede estar adaptado para establecer una clave de sesión secreta compartida con la aplicación. En algunas realizaciones, el lector puede almacenar una clave privada de un par de claves público-privadas y el lector puede estar adaptado para recibir una semilla encriptada por la aplicación con la clave pública de dicho par de claves público-privadas, desencriptar la semilla encriptada, y utilizar la semilla desencriptada para establecer una clave de sesión secreta compartida con la aplicación. En algunas realizaciones, el lector puede estar adaptado para desencriptar o autenticar comandos o datos provenientes de la aplicación (o que pretenden provenir de la aplicación). En algunas realizaciones, el lector puede estar adaptado para verificar firmas o códigos de autenticación de mensajes sobre comandos o datos que pretenden provenir de la aplicación. En algunas realizaciones, el lector puede estar adaptado para encriptar respuestas o datos que devuelve a la aplicación. En algunas realizaciones, el lector puede estar adaptado para utilizar criptografía simétrica con una clave secreta que comparte con la aplicación para desencriptar, encriptar y/o autenticar mensajes y/o datos que el lector intercambia con la aplicación. En algunas realizaciones, el lector puede estar adaptado para utilizar criptografía asimétrica con una clave pública que almacena y que está asociada con el proveedor de aplicación o con una autoridad de certificados fiable para autenticar mensajes, comandos o datos que pretenden provenir de la aplicación (p. ej., al verificar firmas de la aplicación sobre dichos mensajes, comandos o datos). En algunas realizaciones, el lector puede estar adaptado para utilizar criptografía asimétrica con una clave

privada que almacena para autenticar (p. ej., mediante firma) mensajes o datos que devuelve o envía a una aplicación.

En algunas realizaciones, el lector (100) puede estar adaptado para desencriptar o autenticar (es decir, verificar el origen), de esta manera, mensajes de aplicación o datos que se intercambian en el contexto de un protocolo de actualización de firmware seguro. En algunas realizaciones, el lector puede estar adaptado para desencriptar o autenticar de esta manera mensajes de aplicación o datos que se intercambian en el contexto de un protocolo de actualización de parámetros seguro. En algunas realizaciones, el lector puede estar adaptado para desencriptar o autenticar de esta forma datos (o comandos de aplicación que contienen dichos datos) que están concebidos para ser revisados y aprobados por el usuario y/o firmados por la tarjeta.

Identificar al lector.

En algunas realizaciones, el lector puede estar adaptado para permitir la identificación de un lector individual. Por ejemplo, el lector puede almacenar un elemento de datos de identificación (tal y como un número de serie) y puede estar adaptado para permitir que una aplicación obtenga el valor de dicho elemento de datos de identificación (p. ej., a través de algún comando lector). En algunas realizaciones, la identidad del lector puede estar indicada en un certificado de clave pública que está almacenado en el lector y que se puede recuperar mediante una aplicación. En algunas realizaciones, el lector puede almacenar uno o más elementos de datos de identificación que identifican una o más claves públicas almacenadas en el lector y que se pueden recuperar mediante una aplicación. En algunas realizaciones, el lector puede admitir uno o más comandos de lector que permiten que una aplicación recupere los datos de identificación del lector. En algunas realizaciones, el lector incluye los datos de identificación del lector en datos que devuelve en respuesta a otros comandos. Por ejemplo, en algunas realizaciones el lector puede incluir los datos de identificación del lector en la respuesta del lector a una solicitud de aplicación de recuperar la firma del lector sobre un fichero registro.

Intercambio y formato de comandos de lector.

En algunas realizaciones, el lector admite comandos de lector que formalmente presentan el mismo formato o estructura que una APDUs (Unidad de Datos de Protocolo de Aplicación - tal y como se define en la ISO/IEC 7816) de tarjeta inteligente genuina, o que presentan un formato y estructura que es al menos lo suficientemente similar a APDU de tarjeta inteligente genuinas con el fin de que se puedan intercambiar con el lector de la misma manera y utilizando el mismo software y pilas de controladores en el ordenador anfitrión del lector como comandos de tarjeta inteligente genuinos. En algunas realizaciones, el lector puede distinguir comandos de lector de comandos de tarjeta inteligente reales según el contexto o según valores de parámetro de los comandos recibidos. Por ejemplo, en algunas realizaciones, el lector puede reconocer comandos de lector según valores específicos determinados de los bytes CLA y/o INS en una APDU. En algunas realizaciones, el lector puede admitir uno o más comandos que pueden indicar al lector si comandos posteriores se han de interpretar como comandos de tarjeta inteligente o como comandos de lector.

En algunas realizaciones, se pueden utilizar otros mecanismos para intercambiar comandos de lector, p. ej., a través de comandos de USB de uso privado.

Modo desconectado.

En algunas realizaciones, el lector (100) puede estar adaptado para que también pueda funcionar cuando no está conectado a un ordenador anfitrión (99). En tal modo desconectado, puede obtener su energía de su propia fuente de energía autónoma. En el modo desconectado, el lector puede ser capaz de, por ejemplo, funcionar como un testigo de autenticación fuerte y generar contraseñas de uso único, respuestas a puestas a prueba, o firmas de datos de transacciones. Las contraseñas de uso único, respuestas a puestas a prueba y/o firmas de datos de transacción que el lector, por lo tanto, genera en modo desconectado pueden ser generadas por el lector al aplicar un algoritmo que está basado en criptografía simétrica utilizando una clave secreta simétrica que también es conocida por un servidor de verificación. En algunas realizaciones, el lector puede utilizar una tarjeta inteligente (98) insertada para la generación de contraseñas de uso único, respuestas a puestas a prueba y/o firmas de datos de transacciones. En algunas realizaciones, la tarjeta inteligente se puede utilizar para hacer al menos una parte de los cálculos criptográficos para la generación de contraseñas de uso único, respuestas a puestas a prueba y/o firmas de datos de transacciones. En algunas realizaciones, el lector puede utilizar la tarjeta inteligente para obtener un valor que utiliza para derivar la clave secreta simétrica que luego utiliza para la generación de contraseñas de uso único, respuestas a puestas a prueba y/o firmas de datos de transacción. En algunas realizaciones, el lector puede utilizar un valor de tiempo provisto por el reloj (180) para la generación de contraseñas de uso único, respuestas a puestas a prueba y/o firmas de datos de transacciones. En algunas realizaciones, el lector puede utilizar datos que el usuario provee al lector mediante la interfaz de entrada (152) para la generación de respuestas a puestas a prueba y/o firmas de datos de transacciones. En algunas realizaciones, la interfaz de usuario (152) comprende un teclado y el usuario puede teclear los datos. En algunas realizaciones, el lector puede emitir las contraseñas de uso único, respuestas a puestas a prueba y/o firmas de datos de transacciones generadas al usuario a través de la interfaz de salida (151). En algunas realizaciones, la interfaz de salida (151) puede comprender un visualizador y las contraseñas de uso único, respuestas a puestas a prueba y/o firmas de datos de transacciones generadas pueden

visualizarse como una cadena de símbolos, p. ej., una cadena de caracteres decimales, hexadecimales o alfanuméricos.

En algunas realizaciones, el lector (100) puede estar adaptado para ser compatible con el EMV-CAP (Programa de Autenticación de Chip Europay-Mastercard-VISA) o para cumplir con los requisitos EMV-CAP.

Portátil y de mano.

En algunas realizaciones, el lector tiene un peso y medidas espaciales, de modo que el lector pueda considerarse como un dispositivo de mano portátil. En algunas realizaciones, el lector tiene un peso y medidas espaciales, de modo que el lector se pueda enviar al usuario por correo a costes moderados. Por ejemplo, en algunas realizaciones, el lector puede tener un espesor de menos de 2 cm., un ancho de menos de 10 cm., una longitud de menos de 15 cm., y un peso de menos de 200 gramos. En otras realizaciones, el lector puede tener un espesor de menos de 1,5 cm., un ancho de menos de 7 cm., una longitud de menos de 13 cm., y un peso de menos de 110 gramos.

Dispositivo de hardware dedicado.

En algunas realizaciones, el lector es un dispositivo de hardware dedicado. En algunas realizaciones, el lector puede estar dedicado para utilizarse en métodos para asegurar el acceso de un usuario a una aplicación o para asegurar una interacción del usuario con dicha aplicación. En algunas realizaciones, el objetivo principal del lector es que se pueda utilizar para asegurar el acceso de un usuario a una aplicación o para asegurar una interacción del usuario con dicha aplicación. En algunas realizaciones, con el fin de garantizar la dedicación del lector para su uso como un dispositivo de seguridad, el lector puede estar adaptado para que sea imposible alterar su firmware. En algunas realizaciones, con el fin de garantizar la dedicación del lector para su uso como un dispositivo de seguridad, cualquier cambio o actualización de su firmware sólo es posible a través de un protocolo de actualización de firmware seguro que está diseñado para garantizar que sólo una parte fiable de controladora autorizada pueda actualizar o cambiar el firmware del lector. Esto permite a la parte fiable controlada asegurarse de que no se realizará ninguna actualización de firmware que desestime la dedicación del lector a su uso en métodos para asegurar un acceso del usuario a una aplicación o para asegurar una interacción de un usuario con dicha aplicación. Un objeto general del dispositivo con capacidades de lectura de tarjeta inteligente, pero abierto en el sentido de que, por ejemplo, un usuario puede actualizar el software sin autorización de la parte fiable controladora, no se puede considerar un dispositivo dedicado.

Lector seguro.

En algunas realizaciones, el lector de tarjeta inteligente es un lector seguro. Esto significa que la interfaz de entrada del usuario del lector es una interfaz de entrada del usuario segura y que la interfaz de salida del usuario del lector es una interfaz de salida del usuario segura. También significa que los datos y el firmware sensible de seguridad del lector (que pueden comprender claves criptográficas y/o datos de configuración que parametrizan determinadas funciones de seguridad) que no se pueden cambiar ni actualizar, o que sólo se pueden cambiar o actualizar mediante un protocolo de actualización seguro que sólo permite que una parte fiable lleve a cabo el cambio o actualización.

La Figura 2 ilustra un sistema para realizar transacciones seguras según un aspecto de la invención. El sistema comprende un lector (100) de tarjeta inteligente, tal y como un lector descrito en conexión con la Figura 1, un ordenador anfitrión (99) al que el lector (100) de tarjeta inteligente puede estar conectado, uno o más servidores de aplicaciones remotos (200), y una red informática (210) que puede conectar el ordenador anfitrión (99) y uno o más servidores de aplicaciones remotos (200). El sistema además comprende una tarjeta inteligente (98) asociada con un usuario que puede insertarse en el lector (100) de tarjeta inteligente.

El ordenador anfitrión (99) puede comprender una interfaz de usuario, tal y como un visualizador y un teclado y un ratón para interactuar con un usuario. El ordenador anfitrión (99) puede comprender una interfaz de red para conectar el ordenador anfitrión (99) a una red informática (210). El ordenador anfitrión (99) puede comprender medios de procesamiento de datos, tal y como un microprocesador. El ordenador anfitrión (99) puede comprender una memoria. El ordenador anfitrión (99) puede comprender un software, tal y como un sistema operativo y un software de aplicación. En una realización típica, el ordenador anfitrión (99) puede comprender un PC (ordenador personal) o un portátil. El ordenador anfitrión (99) puede comprender una interfaz para intercambiar datos y/o comandos y/o respuestas con hardware periféricos, tal y como, por ejemplo, el lector (100) de tarjeta inteligente. Esta interfaz puede, por ejemplo, comprender una interfaz de USB.

El servidor de aplicaciones remoto (200) puede comprender un servidor web. El servidor de aplicaciones remotas puede comprender múltiples componentes de software que se ejecutan en múltiples componentes de hardware. El servidor de aplicaciones remotas puede interactuar con el software en el ordenador anfitrión. El servidor de aplicaciones remotas y/o software en el ordenador anfitrión pueden ser componentes de una aplicación total. En algunas realizaciones, algunos componentes, tal y como una aplicación total, pueden estar operados por o en representación de diferentes agentes. Por ejemplo, en algunas realizaciones, la aplicación total puede comprender

componentes que funcionan mediante o en representación de un usuario o cliente, otros componentes que funcionan mediante o en representación de un proveedor, y/o incluso otros componentes que funcionan mediante o en representación de una entidad financiera. Uno o más de los servidores de aplicaciones remotas pueden comprender más de un servidor de aplicaciones remotas mediante los cuales diferentes servidores pueden quedar a cargo de diferentes funciones. Por ejemplo, en algunas realizaciones, el usuario puede interactuar con un servidor para enviar datos de transacción a una aplicación, mientras que otro servidor puede ser responsable de verificar la tarjeta y/o las firmas de lector sobre, por ejemplo, los datos de transacción.

La red informática (210) puede, por ejemplo, comprender Internet.

En algunas realizaciones, la tarjeta inteligente (98) puede, por ejemplo, comprender una tarjeta inteligente PKI capaz de generar firmas utilizando criptografía asimétrica con la clave privada de un par de claves público-privadas. La tarjeta inteligente (98) puede almacenar y utilizar de forma segura la clave privada de un par de claves público-privadas. La tarjeta inteligente (98) puede también almacenar una clave pública de un par de claves público-privadas y/o un certificado asociado con la clave pública de un par de claves público-privadas. Las funciones que utilizan la clave privada de un par de claves público-privadas en la tarjeta inteligente (98) pueden estar protegidas por un PIN.

En algunas realizaciones, la tarjeta inteligente (98) puede, por ejemplo, comprender una tarjeta inteligente capaz de generar criptogramas utilizando criptografía simétrica con una clave secreta. La tarjeta inteligente (98) puede almacenar y utilizar de forma segura la clave secreta. Las operaciones que utilizan la clave secreta almacenada en la tarjeta inteligente (98) pueden estar protegidas por un PIN. En algunas realizaciones, la tarjeta inteligente (98) puede ser compatible con EMV, o cumplir con los requisitos EMV, o puede comprender una aplicación de tarjeta inteligente compatible con EMV o que cumpla con los requisitos EMV.

En algunas realizaciones, una aplicación a la que el usuario accede a través del ordenador anfitrión y que interactúa con el lector (100) de tarjeta inteligente para asegurar el acceso a la aplicación del usuario, puede ejecutarse a través de o albergarse en el servidor de aplicaciones remotas (200). En algunas realizaciones, partes de esta aplicación pueden ejecutarse a través de albergarse en el servidor de aplicaciones remotas (200) y partes de la aplicación pueden ejecutarse a través de o albergarse en el ordenador anfitrión (99). En algunas realizaciones, la aplicación puede ejecutarse a través de o albergarse en el ordenador anfitrión (99) y el servidor de aplicaciones remotas (200), en cuyo caso la red informática (210) puede ser opcional o inexistente. En algunas realizaciones, algunos componentes de la aplicación pueden funcionar mediante o en representación de diferentes agentes. Por ejemplo, en algunas realizaciones, la aplicación puede comprender componentes que funcionan mediante o en representación de un usuario o cliente, otros componentes que funcionan mediante o en representación de un proveedor, y/o incluso otros componentes que funcionan mediante o en representación de una entidad financiera.

En algunas realizaciones, la aplicación puede comprender una aplicación de banca por Internet o web bancaria, el servidor de aplicaciones remotas (200) puede comprender un servidor web que puede ser una entrada web de un servidor bancario final y el ordenador anfitrión (99) puede estar conectado al servidor web a través de Internet (210) y puede comprender un navegador web que el usuario puede utilizar para acceder a la aplicación bancaria web a través de Internet (210).

Las Figuras 3a y 3b ilustran un método según un aspecto de la invención para asegurar transacciones remotas.

Proveer un lector a un usuario.

En la etapa (302), se puede ofrecer a un usuario un lector (100) de tarjeta inteligente seguro, tal y como un lector descrito en conexión con la Figura 1. En algunas realizaciones, un dueño de la aplicación provee un lector apropiado para uno o más usuarios de la aplicación. En algunas realizaciones, una aplicación anima a los usuarios de la aplicación a que obtengan un lector apropiado. En algunas realizaciones, una aplicación provee información a los usuarios de la aplicación acerca de cómo obtener un lector apropiado.

Conectar el lector con el ordenador anfitrión del usuario.

En la etapa (304), un lector (100) de tarjeta inteligente seguro que se puede haber otorgado al usuario se conecta a un ordenador anfitrión (99) que el usuario puede utilizar.

El usuario que accede a la aplicación.

En la etapa (306), el usuario accede a una aplicación utilizando un ordenador anfitrión (99) al que se puede conectar el lector (100) de tarjeta inteligente seguro. En algunas realizaciones, la aplicación puede, por ejemplo, comprender una aplicación albergada por un servidor de aplicaciones remotas (200). En otras realizaciones, la aplicación puede comprender una aplicación de software ejecutada por el ordenador anfitrión. En incluso otras realizaciones, la aplicación puede comprender una aplicación cliente-servidor que comprende un módulo de software de cliente que se ejecuta en el ordenador anfitrión y uno o más módulos de software de servidor que se ejecutan en uno o más servidores remotos (200). En una realización, la aplicación puede comprender un editor de texto. En otra realización, la aplicación puede comprender un programa de correo electrónico. En incluso otra realización, la aplicación puede comprender una aplicación financiera, tal y como una aplicación bancaria de Internet. En una realización, el usuario

puede acceder a una aplicación basada en entorno web remota utilizando un navegador web que se ejecuta en su ordenador anfitrión.

El usuario que inicia una transacción.

En la etapa (308), el usuario puede interactuar con la aplicación, p. ej., en el ordenador anfitrión o en un servidor remoto, por ejemplo, para iniciar una transacción. Durante la interacción del usuario con la aplicación, el usuario puede enviar una transacción a la aplicación. Por ejemplo, el usuario puede proveer a un sitio web bancario de Internet los detalles de una transferencia de dinero que el usuario desea realizar, o el usuario puede indicar su deseo de comprar determinados artículos en un sitio web comercial, o el usuario puede aprobar un contrato o puede escribir un correo electrónico o una carta a firmar.

Recolección de datos a firmar.

En la etapa (310), la aplicación, p. ej., en el ordenador anfitrión o en un servidor remoto, recolecta un conjunto de datos para que el usuario firme de manera digital, p. ej., datos representativos de la transacción iniciada por el usuario. Este conjunto de datos puede, por ejemplo, comprender un documento o un correo electrónico a firmar o puede, por ejemplo, comprender datos representativos o relacionados con una transacción financiera que el usuario desea realizar. Los datos a firmar pueden, por ejemplo, comprender datos relacionados con una transferencia de dinero que el usuario desea realizar, tal y como, por ejemplo, la cantidad de dinero a transferir, un indicador de moneda, una indicación del destino (p. ej., un número de cuenta de destino) al que el dinero se debe transferir, y/o una indicación del origen (p. ej. el número de cuenta origen) desde el cual se debe tomar el dinero a transferir. En otro caso, los datos a firmar pueden, por ejemplo, estar relacionados con una orden de valores, tal y como, por ejemplo, la venta o adquisición de un número de acciones. Los datos pueden, por ejemplo, comprender un indicador del tipo de acciones a comerciar, un indicador del número de acciones a comerciar, el tipo de comercio (vender, comprar,...), el precio, período de validez,...

Inserción de la tarjeta inteligente.

En un punto (312), al usuario se le solicita que ingrese la tarjeta inteligente del usuario en el lector y el usuario inserta la tarjeta inteligente en el lector. A partir de este momento, la aplicación y el lector pueden comenzar a intercambiar comandos de tarjeta inteligente con la tarjeta inteligente insertada. En algunas realizaciones, insertar una tarjeta inteligente implica insertar físicamente una tarjeta inteligente en la ranura de tarjeta inteligente del lector. En otras realizaciones (p. ej., en realizaciones en donde el lector interactúa con una tarjeta inteligente sin contacto utilizando un protocolo de comunicación de tarjeta inteligente sin contacto), insertar la tarjeta inteligente significa posicionar la tarjeta inteligente con respecto al lector de manera que la comunicación entre la tarjeta inteligente y el lector de tarjeta inteligente sea posible. Por ejemplo, en algunas realizaciones no es necesario insertar físicamente la tarjeta inteligente en el lector, sino que la tarjeta inteligente debe estar dentro de un determinado intervalo de distancia (p. ej. a menos de 10 cm.) para que la comunicación sea posible.

Identificar al lector.

En la etapa (314), la aplicación, p. ej. en el ordenador anfitrión o en un servidor remoto, identifica al lector. En algunas realizaciones, la aplicación simplemente establece el tipo de lector. En otras realizaciones, la aplicación obtiene una versión del firmware del lector. En incluso otras realizaciones, la aplicación obtiene una indicación de la identidad del lector particular (p. ej. un número de serie del lector o una referencia a una clave pública correspondiente a una clave privada almacenada en el lector). En algunas realizaciones, la aplicación puede utilizar mecanismos de lector de tarjeta inteligente USB estándares para recuperar el tipo de lector. En otras realizaciones, la aplicación puede utilizar uno o más comandos de lector para recuperar los datos de identificación del lector. En algunas realizaciones, la aplicación puede recuperar los datos de identificación del lector como parte de un conjunto de datos del lector que también puede comprender otros datos relacionados con el lector, tal y como el estado del lector, el conjunto de datos de configuración del lector, la versión de firmware del lector, etc.

El lector entra en modo de registro seguro.

En la etapa (320), el lector de tarjeta inteligente está fabricado para entrar en un modo de registro seguro. En algunas realizaciones, el lector puede entrar en el modo de registro seguro en respuesta a un comando de lector específico que instruye al lector para que entre en el modo de registro seguro. En algunas realizaciones, el lector puede entrar en el modo de registro seguro como un efecto secundario automático de un comando de lector que instruye al lector para que lleve a cabo una acción, tal y como un comando para autenticar el usuario de una forma segura (por ejemplo, mediante el ingreso de PIN seguro) o un comando para presentar determinados datos al usuario para su aprobación o revisión o un comando para llevar a cabo una sesión de firma segura. En algunas realizaciones, el lector puede entrar en el modo de registro seguro automáticamente en respuesta a un determinado evento, tal y como un evento de encendido del lector o un evento de inserción de tarjeta inteligente o un evento de reinicio o encendido de tarjeta inteligente. En algunas realizaciones, el lector puede estar, por defecto, en un modo de registro seguro. En algunas realizaciones, el lector está siempre en un modo de registro seguro. En algunas realizaciones, el lector inicializará uno o más ficheros de registro en un estado particular. Por ejemplo, pueden

reiniciarse para estar vacíos o pueden inicializarse con un conjunto de datos que puede, por ejemplo, comprender datos de configuración (por ejemplo, datos de configuración que afectan el modo de registro seguro) y/o datos indicativos del estado de lector y/o versión de firmware, etc. En algunas realizaciones, esta inicialización puede suceder antes de que el lector sea puesto en el modo de registro seguro. En algunas realizaciones, esta inicialización puede suceder cuando el lector entra en el modo de registro seguro. En algunas realizaciones, esto puede suceder en algún punto posterior a que el lector entre en el modo de registro seguro.

El lector registra datos.

Una vez en el modo de registro seguro, el lector de tarjeta inteligente puede comenzar a agregar datos automáticamente a uno o más ficheros de registro (etapa 321). En algunas realizaciones, los datos agregados a los ficheros de registro comprenden datos representativos de acciones, estados y eventos sensibles de seguridad, tal y como comandos y/o respuestas de lector, interacciones de usuario (p. ej. presentación de datos al usuario y entrada del usuario) con el lector, comandos y/o respuestas de tarjeta inteligente, versión de firmware y/o eventos de cambio de firmware, datos de configuración y/o eventos de cambio de datos de configuración, otros eventos (p. ej. eventos que pueden ser indicativos de intentos de manipulación o que pueden comprometer la integridad de la seguridad del lector, tal y como, la detección de determinadas manipulaciones mecánicas o electrónicas, tal y como intentos de abrir el alojamiento o picos de tensión o pérdidas de tensión...).

El lector registra comandos de tarjeta inteligente.

En algunas realizaciones, el lector registra de esta manera datos relacionados con comandos de tarjeta inteligente que intercambia con la tarjeta, por ejemplo, comandos de tarjeta inteligente transparente que el lector recibe de una aplicación para intercambiarlos con una tarjeta inteligente insertada en el lector (etapa 322). En algunas realizaciones, el lector puede registrar sistemáticamente todos los comandos de tarjeta inteligente intercambiados. En algunas realizaciones, el lector puede registrar solo algunos comandos de tarjeta inteligente intercambiados. En algunas realizaciones, el lector puede registrar aquellos comandos de tarjeta inteligente que cumplan con determinados criterios. Por ejemplo, el lector puede registrar comandos de tarjeta inteligente de un determinado tipo. En algunas realizaciones, los criterios que el lector utiliza para decidir qué comandos registra pueden estar parametrizados por parámetros de configuración. Estos parámetros de configuración pueden, por ejemplo, comprender una relación de comandos a registrar o una relación de comandos que no deben registrarse. En algunas realizaciones, el lector puede reconocer los tipos de comandos de tarjeta inteligente en base a los valores de ciertos bytes de la cabecera de comando de tarjeta inteligente, tal y como, por ejemplo, los bytes CLA, INS, P1 y/o P2. En algunas realizaciones, los parámetros de configuración que determinan qué comandos de tarjeta inteligente (y/o sus correspondientes respuestas de tarjeta) se registrarán y, si fuese aplicable, en qué fichero de registro, se comunican al lector mediante la aplicación, por ejemplo, mediante algún comando de lector, p. ej. un comando de lector que instruya al lector para que entre en un modo de registro seguro.

El lector registra comandos de lector.

En algunas realizaciones, el lector registra datos relacionados con comandos de lector que recibe (etapa 323). En algunas realizaciones, el lector puede registrar sistemáticamente todos los comandos de lector intercambiados. En algunas realizaciones, el lector puede registrar solo algunos comandos de lector intercambiados.

Establecer parámetros de configuración de registro seguro.

En algunas realizaciones, la aplicación instruye al lector mediante un comando de lector para que entre en el modo de registro seguro y pase (etapa 316) al lector, mediante el mismo comando de lector o uno o más comandos de lector extra, un conjunto de parámetros de configuración del modo de registro seguro que puede determinar qué datos debe registrar el lector en el modo de registro seguro, tal y como, por ejemplo, qué comandos de tarjeta inteligente registrar, qué comandos de lector registrar, qué interacciones de usuario registrar (p. ej. qué mensajes y/o datos del usuario el lector presenta al usuario y qué respuestas del usuario recibe el lector del usuario), qué otros eventos (p. ej. eventos de error) registrar. En algunas realizaciones, el lector automáticamente registra los parámetros de configuración pertinentes y/o cualquier cambio en estos parámetros de configuración. En algunas realizaciones, la aplicación puede pasar parámetros de configuración del modo de registro seguro al lector mediante uno o más comandos de lector. En algunas realizaciones, el lector puede pasar parámetros de configuración del modo de registro seguro al lector mediante el mismo comando de lector que instruye al lector para que entre en el modo de registro seguro. En algunas realizaciones, la aplicación utiliza uno o más comandos de lector distintos para pasar parámetros de configuración del modo de registro seguro al lector. En algunas realizaciones, el lector puede pasar parámetros de configuración del modo de registro seguro al lector antes de que el lector entre en el modo de registro seguro. En algunas realizaciones, el lector puede pasar parámetros de configuración del modo de registro seguro al lector después de que el lector entre en el modo de registro seguro.

Registrar revisión y aprobación de datos de transacción.

Algunas realizaciones hacen que el lector, cuando se encuentra en modo de registro seguro, registre (etapa 324) al menos datos (o una representación de dichos datos, como un resumen o un troceado de dichos datos) que el lector

presenta al usuario y que el usuario revisa y aprueba (o desaprueba). En algunas realizaciones, el lector registra los datos que presenta para revisión y aprobación y registra la decisión del usuario (aprobación o rechazo). En algunas realizaciones, el lector registra solo los datos que se han presentado al usuario y que el usuario ha revisado y aprobado (y el lector no registra datos que el usuario ha rechazado). En algunas realizaciones, el lector registra los comandos de lector (o una representación de dichos comandos, tal y como, un troceado de los comandos de lector o partes de los comandos de lector) que la aplicación utiliza para comunicar al lector los datos a revisar y aprobar y registra las respuestas del lector a la aplicación para indicar la aprobación o rechazo del usuario.

Algunas realizaciones hacen que el lector, cuando se encuentra en modo de registro seguro, al menos registre (etapa 336) datos (o una representación de dichos datos, como un resumen o un troceado, o incluso una firma de tarjeta sobre estos datos) que la aplicación envía a la tarjeta para su firma. En algunas realizaciones, esto se puede llevar a cabo al registrar el lector los contenidos del comando de tarjeta inteligente que se utilizan para pasar a la tarjeta los datos a firmar. En algunas realizaciones, esto se lleva a cabo al registrar la respuesta de la tarjeta que contiene la firma de la tarjeta sobre los datos a firmar. Algunas realizaciones hacen que el lector registre todos los comandos de tarjeta inteligente que una aplicación puede utilizar para permitir que la tarjeta firme datos. En algunas realizaciones, el lector registra todos los comandos de tarjeta inteligente transparente que la aplicación envía a la tarjeta a través del lector cuando el lector se encuentra en modo de registro seguro. En algunas realizaciones, el lector registra todos los comandos de tarjeta inteligente transparente que la aplicación envía a la tarjeta a través del lector cuando el lector se encuentra en modo de registro seguro y que cumplen determinados criterios. En algunas realizaciones, estos criterios son parte de los datos de configuración del lector para el modo de registro seguro. En algunas realizaciones, estos criterios pueden establecerse de manera que se garantice que aquellos comandos de tarjeta inteligente están registrados, que indique o determine qué datos firmó o firmará la tarjeta. En algunas realizaciones, el lector registra una firma de tarjeta inteligente sobre los datos a firmar además o a cambio de los datos a firmar por ellos mismos.

Algunas realizaciones hacen que el lector, cuando se encuentra en modo de registro seguro, al menos registre tanto los datos (o una representación de dichos datos) que el lector presenta al usuario (tal y como se describe antes) y que el usuario revisa y aprueba, como los datos (o representación de dichos datos) que la aplicación envía a la tarjeta para su firma (tal y como se describe antes).

Registrar datos según criterios

En algunas realizaciones, el lector está adaptado para registrar cualquier evento, comando de tarjeta inteligente transparente, comando de lector, acción del usuario u otro evento que cumpla con determinados criterios. En algunas realizaciones, estos criterios pueden ser parte de los datos de configuración del lector. En algunas realizaciones, la aplicación puede, en la etapa (316), establecer o cambiar al menos algunos de los datos de configuración del lector. Por ejemplo, en algunas realizaciones, la aplicación puede instruir al lector para que entre en modo de registro seguro y aplique determinados datos de configuración que pueden comprender algunos de los criterios que el lector puede utilizar para decidir qué eventos, comandos de tarjeta inteligente, acciones del lector o acciones del usuario registra.

Registrar datos de configuración.

En algunas realizaciones, el lector registra (etapa 318) automáticamente todos o parte de los datos de configuración que aplica para decidir qué registrar. En algunas realizaciones, el lector registra automáticamente los datos de configuración que recibe de la aplicación y que aplica para decidir qué registrar.

Intercambiar comandos de tarjeta inteligente transparente.

En la etapa (328), la aplicación envía una serie de uno o más comandos de tarjeta transparente al lector de tarjeta inteligente seguro para que el lector intercambie con la tarjeta inteligente insertada en el lector de tarjeta inteligente y devuelva las respuestas de tarjeta a estos comandos de tarjeta inteligente a la aplicación. En algunas realizaciones, la aplicación intercambia estos comandos con el lector a través de pilas de software estándar en el ordenador anfitrión del lector para intercambiar comandos de tarjeta inteligente con una tarjeta inteligente insertada en un lector de tarjeta inteligente. En algunas realizaciones, esta pila de software puede comprender un controlador USB de CCID (dispositivo de interfaz de tarjeta de circuito integrado) y/o un componente PC/SC (ordenador personal/tarjeta inteligente). Tal y como se indicó anteriormente, en algunas realizaciones, el lector puede, cuando se encuentra en modo de registro seguro, agregar datos relacionados con todos o parte de estos comandos de tarjeta inteligente y/o las correspondientes respuestas de tarjeta a uno o más de los ficheros de registro del lector. En algunas realizaciones, el lector puede admitir una interfaz de contacto y puede intercambiar comandos con una tarjeta inteligente a través de contactos galvánicos. En algunas realizaciones, el lector puede admitir una interfaz de tarjeta inteligente sin contacto y puede intercambiar comandos con una tarjeta inteligente utilizando un protocolo de comunicación sin contacto, tal y como, por ejemplo, el protocolo ISO/IEC 14443. En algunas realizaciones, el lector de tarjeta inteligente comprende una ranura de tarjeta inteligente para insertar una tarjeta inteligente.

Aplicar cortafuegos a comandos de tarjeta inteligente.

En algunas realizaciones, el lector puede someter (etapa 326) estos comandos de tarjeta inteligente a un cortafuegos antes de intercambiarlos con la tarjeta inteligente. En algunas realizaciones, el lector puede bloquear algunos comandos de tarjeta inteligente basados en determinados criterios.

En algunas realizaciones, la aplicación puede, por ejemplo, intercambiar comandos de tarjeta inteligente transparente con la tarjeta inteligente para seleccionar una función en la tarjeta para generar firmas y/o seleccionar un perfil o entorno de seguridad en la tarjeta y/o leer datos de la tarjeta, tal y como, por ejemplo, datos relacionados con el usuario y/o claves públicas asociadas con el usuario (por ejemplo, un certificado).

Verificar identidad del usuario

En la etapa (330), el lector puede verificar la identidad del usuario. Por ejemplo, el lector puede llevar a cabo un ingreso de PIN seguro. El lector puede solicitar al usuario que ingrese un PIN, capturar el PIN que el usuario ingresa, y enviar el PIN a la tarjeta inteligente para que lo verifique la tarjeta inteligente. En algunas realizaciones, la aplicación instruye al lector para que lleve a cabo un ingreso de PIN seguro mediante uno o más comandos de lector de ingreso de PIN seguro. En otras realizaciones, el lector verifica la identidad del usuario mediante un método de autenticación del usuario biométrica que puede, por ejemplo, estar basado en huellas digitales. En algunas realizaciones, el lector puede registrar la verificación de la identidad del usuario. Por ejemplo, el lector puede registrar si se realizó la verificación de la identidad del usuario y/o cuál fue el resultado de la verificación de la identidad del usuario.

Aprobación de datos de transacción.

En la etapa (331), la aplicación envía datos (p. ej. datos de transacción) al lector para presentarlos al usuario para que el usuario los revise y apruebe. En algunas realizaciones, la aplicación utiliza comandos de lector específicos para enviar estos datos al lector. El lector puede presentar estos datos al usuario (p. ej. al presentar los datos en el visualizador del lector) y solicitar al usuario que revise los datos y que indique su aprobación o rechazo. El lector puede capturar (332) la aprobación o rechazo del usuario (que el usuario puede, por ejemplo, indicar al presionar un botón de Aceptar o Cancelar). El lector puede devolver a la aplicación la decisión de aprobación o rechazo del usuario. En algunas realizaciones, la aplicación puede abortar la transacción si el usuario no aprueba los datos.

En realizaciones típicas, el lector registra (333) los datos presentados a y/o aprobados por el usuario (o una representación de estos datos, tal y como, por ejemplo, un resumen o troceado). En algunas realizaciones, el lector solo registra los datos si el usuario los aprueba. En algunas realizaciones, el lector registra los datos independientemente de si el usuario los aprobó o rechazó y también registra la decisión del usuario (es decir, si el usuario aprobó o rechazó los datos). En algunas realizaciones, el lector registra los datos y un elemento de datos que indica el resultado del usuario. En algunas realizaciones, el lector solo registra los datos que han sido revisados si el usuario los aprobó, por lo que el hecho de que el lector registrara estos datos es una indicación en el fichero de registro de que el usuario revisó y aprobó estos datos. En estas realizaciones, el lector registra el/los comando/s de lector que contiene/n los datos a revisar y aprobar por el usuario y también registra la/s respuesta/s correspondiente/s que contiene/n una indicación de la decisión del usuario.

Firma de los datos de transacción por parte de la tarjeta.

En la etapa (334), si el usuario ha aprobado los datos, se hace que la tarjeta inteligente firme un conjunto de datos. En una realización típica, la aplicación puede generar un resumen sobre los datos a firmar (p. ej. aplicando una función de troceado criptográfico a los datos) y puede enviar el resumen o troceado a la tarjeta inteligente a partir de lo cual la tarjeta inteligente firma el resumen o troceado enviado. En algunas realizaciones, la aplicación puede enviar los datos a firmar directamente a la tarjeta inteligente. En algunas realizaciones, la tarjeta inteligente puede generar un resumen o troceado sobre los datos a firmar que recibió de la aplicación y firmar dicho resumen o troceado. En algunas realizaciones, los datos a firmar y los datos a revisar y aprobar por el usuario son idénticos. En algunas realizaciones, los datos a firmar comprenden los datos a revisar y aprobar, pero también pueden comprenden otros datos (tal y como, por ejemplo, una puesta a prueba aleatoria que no tiene significado alguno para el usuario y que, por lo tanto, no requiere revisión y aprobación, pero que puede servir para prevenir determinados tipos de ataques de reproducción). En algunas realizaciones, los datos a revisar y aprobar comprenden los datos a firmar, pero también pueden comprender información adicional que no se envió a la tarjeta para su firma. En realizaciones típicas, hay al menos una superposición parcial entre, por un lado, los datos a revisar y aprobar y, por el otro, los datos a firmar. En algunas realizaciones, sin embargo, no hay una superposición literal directa entre, por un lado, los datos a revisar y aprobar y, por el otro, los datos a firmar, pero puede haber una relación, p. ej. con respecto al significado de estos datos. Por ejemplo, los datos a firmar pueden comprender un contrato completo y los datos a revisar y aprobar pueden comprender un breve resumen del contrato.

En realizaciones típicas, la aplicación envía los datos a firmar mediante comandos de tarjeta inteligente transparente que intercambia con la tarjeta inteligente. En dichas realizaciones, el lector puede no tener conocimiento o no requerir conocimiento respecto del conjunto de comandos que se pueden utilizar para permitir que una tarjeta firme datos a firmar. Por ejemplo, en algunas realizaciones, la aplicación puede enviar un comando de tarjeta inteligente transparente a la tarjeta inteligente para seleccionar el entorno de seguridad apropiado (que puede, p. ej.,

seleccionar la clave privada que la tarjeta utilizará posteriormente). La aplicación puede enviar uno o más comandos de tarjeta inteligente transparente a la tarjeta inteligente para enviar a la tarjeta inteligente un resumen o troceado de los datos a firmar, o la aplicación puede enviar uno o más comandos de tarjeta inteligente transparente a la tarjeta inteligente para enviar a la tarjeta inteligente los datos a firmar por sí mismos y la tarjeta inteligente puede calcular un resumen o troceado (p. ej. automáticamente o al recibir un comando explícito de la aplicación para hacerlo). La tarjeta inteligente puede entonces firmar el resumen o troceado recibido o generado. En algunas realizaciones, se utiliza el mismo comando de tarjeta inteligente al mismo tiempo para enviar a la tarjeta inteligente los datos a firmar o un resumen o troceado sobre los datos a firmar e instruir a la tarjeta inteligente para que genere la firma real. En otras realizaciones, se pueden utilizar diferentes comandos de tarjeta inteligente para, por un lado, enviar a la tarjeta inteligente los datos a firmar o un resumen o troceado sobre los datos a firmar y, por el otro, instruir a la tarjeta inteligente para que genere la firma real. En algunas realizaciones, se pueden conocer todos o parte de estos comandos de tarjeta inteligente relacionados con la generación de firmas sobre datos como "comandos PSO" (realizar operación de seguridad).

En otras realizaciones, la aplicación utiliza comandos de lector de firma seguros que instruyen al lector para que presente determinados datos al usuario para su revisión y aprobación y (si el usuario aprueba los datos) para que envíe los datos aprobados (o un conjunto de datos relacionados con los datos aprobados) a la tarjeta inteligente para su firma. En dichas realizaciones, el lector puede tener conocimiento integrado o configurado respecto del conjunto de comandos que se pueden utilizar para permitir que una tarjeta firme datos a firmar con el fin de que pueda construir los comandos correctos. En algunas realizaciones, la aplicación puede pasar al lector información acerca de cómo construir los comandos de firma.

Registrar datos firmados por la tarjeta.

En realizaciones típicas, el lector registra, en la etapa (336), los datos (o datos representativos de estos datos, tal y como un resumen o troceado) que han sido firmados por la tarjeta. En algunas realizaciones, el lector registra todos los comandos de tarjeta inteligente transparente (al menos durante un tiempo determinado) con el fin de que también se registre automáticamente cualquier comando de tarjeta inteligente transparente que la aplicación utilice para enviar datos a la tarjeta para su firma. En algunas realizaciones, el lector está configurado para registrar automáticamente todos los comandos de tarjeta inteligente transparente que cumplan con determinados criterios, y estos criterios están configurados con el fin de que también se registre automáticamente cualquier comando de tarjeta inteligente transparente que la aplicación utilice para enviar datos a la tarjeta para su firma. En realizaciones típicas, el lector no tiene conocimiento acerca de cómo reconocer comandos de tarjeta inteligente que se utilizan para enviar a la tarjeta los datos a firmar. En algunas realizaciones, el lector también registra las respuestas de tarjeta que corresponden a los comandos de tarjeta inteligente que se están registrando. En algunas realizaciones, algunos comandos de tarjeta inteligente se pueden registrar sin las correspondientes respuestas de tarjeta. En algunas realizaciones, algunas respuestas de tarjeta se pueden registrar sin los correspondientes comandos de tarjeta inteligente. En algunas realizaciones, el lector solo registra los datos a firmar (o una representación de los mismos, tal y como un troceado). En algunas realizaciones, el lector solo registra la firma de la tarjeta (que puede considerarse como una representación de los datos a firmar). En algunas realizaciones, el lector registra tanto los datos a firmar (o una representación de los mismos, tal y como un troceado) como la correspondiente firma de la tarjeta.

Recuperar firma de tarjeta.

En la etapa (338), la aplicación recupera la firma de tarjeta que la tarjeta generó sobre los datos a firmar, p. ej. al recibir la respuesta de tarjeta a un comando de tarjeta inteligente de firma.

Generar firma de lector sobre fichero/s de registro.

En la etapa (340), el lector genera firmas de lector sobre los datos registrados. En algunas realizaciones, el lector genera la firma de registro utilizando un algoritmo de firma basado en criptografía asimétrica y utilizando una clave privada de lector de un par de claves público-privadas mediante lo cual dicha clave privada se almacena de forma segura en el lector. En algunas realizaciones, el lector genera la firma de registro utilizando un algoritmo basado en criptografía simétrica y utilizando una clave de lector secreta almacenada de forma segura en el lector y mediante lo cual la clave de lector secreta se puede compartir con determinado servidor de verificación. En una realización típica, todos los datos registrados se registran en un único fichero de registro y el lector genera una única firma de registro sobre ese único fichero de registro. En algunas realizaciones, el lector puede utilizar múltiples ficheros de registro para registrar datos y puede firmar algunos ficheros de registro de forma separada, con el fin de que la firma de registro comprenda las múltiples firmas sobre los ficheros de registro firmados de forma separada. Por ejemplo, en algunas realizaciones, el lector puede registrar comandos o datos de lector para revisión y aprobación en un fichero de registro y puede registrar comandos de tarjeta inteligente transparente en otro fichero de registro y generar firmas sobre cada uno de estos ficheros de registro, con el fin de que la firma de registro del lector comprenda tanto la firma de lector sobre el fichero de registro con los comandos o datos de lector registrados para revisión y aprobación y la firma de lector sobre el fichero de registro con los comandos de tarjeta inteligente transparente.

Recuperar la firma de lector generada.

En la etapa (342), la aplicación recupera la/s firma/s de lector que el lector generó sobre uno o más registros. En algunas realizaciones, la aplicación también puede recuperar los contenidos de los registros firmados de los mismos. En algunas realizaciones, la aplicación también puede recuperar del lector uno o más certificados relacionados con una o más claves (que pueden comprender claves privadas de pares de claves público-privadas) que el lector utilizó para generar la firma de lector sobre el registro. En algunas realizaciones, la aplicación también puede recuperar del lector una o más claves públicas que corresponden a claves privadas de pares de claves público-privadas que el lector utilizó para generar la firma de lector sobre el registro. En algunas realizaciones, la aplicación también puede recuperar del lector datos de identificación que la aplicación puede utilizar para obtener (p. ej. consultando una base de datos) una o más claves públicas y/o certificados relacionados con una clave utilizada por el lector para generar una firma de lector sobre un fichero de registro.

Verificación de que el usuario ha aprobado de hecho la transacción.

Después de que los datos de transacción se han enviado a la aplicación y que el usuario ha revisado los datos a revisar y aprobar y que la tarjeta ha firmado los datos a firmar, la aplicación puede verificar si todo ocurrió según las políticas de seguridad aplicables de la aplicación. Por ejemplo, con el fin de excluir o minimizar el riesgo de un ataque de intermediarios mediante el cual un atacante interfiere con la transacción al reemplazar los datos de transacción que el usuario pretendía enviar a la aplicación con datos fraudulentos (p. ej. un atacante puede haber cambiado el número de cuenta de destino en una transacción de transferencia de dinero), la aplicación puede verificar si los datos de transacción que el usuario envió a la aplicación efectivamente corresponden a los datos que el usuario revisó y aprobó en el lector seguro y firmó con la tarjeta. Para poder realizar esta verificación, la aplicación puede verificar la firma de tarjeta y la firma de lector en el fichero de registro y verificar si los contenidos de el/los fichero/s de registro firmado/s corresponde/n a los eventos que deberían haber ocurrido según las expectativas y políticas de seguridad de la aplicación. En una realización típica, las políticas de seguridad de la aplicación requieren que una representación de los datos de transacción que se revisan y aprueban por el usuario en el lector seguro y que una representación de los mismos datos de transacción estén firmados por la tarjeta. En algunas realizaciones, la aplicación puede además requerir que la revisión y aprobación del usuario y la firma de tarjeta sucedan en la misma sesión. En algunas realizaciones, la aplicación puede además requerir que en la sesión no se presente ningún otro dato al usuario para revisión y aprobación y/o que la tarjeta no firme ningún otro dato. En una realización típica, el lector está configurado para registrar todos los datos revisados y las aprobaciones de datos por el usuario en el lector y para registrar todos los datos firmados por la tarjeta (p. ej. al registrar un conjunto de comandos de tarjeta inteligente transparente que puede comprender todos los comandos de tarjeta inteligente). En algunas realizaciones, la aplicación requiere que los datos de transacción enviados y los datos revisados y aprobados por el usuario en el lector y los datos firmados por la tarjeta sean los mismos. En algunas realizaciones, la aplicación no requiere que estos datos sean idénticos, pero sí requiere que exista cierta relación predefinida entre ellos. Por ejemplo, en algunas realizaciones, los datos revisados por el usuario pueden comprender un subconjunto o compendio de los datos de transacción enviados o de los datos firmados por la tarjeta. Por ejemplo, los datos firmados por la tarjeta pueden comprender, además de los datos revisados por el usuario, algunos elementos de datos (tal y como una número de secuencia de transacción) que pueden no tener significado para el usuario y que, por lo tanto, no se presentan al usuario para revisión. Por ejemplo, los datos de transacción enviados pueden comprender datos de transacción variables junto con una relación voluminosa de términos y condiciones estándar y sólo los datos de transacción variables se presentan de forma efectiva al usuario para su revisión en el lector seguro.

En las siguientes etapas de ejemplo, la aplicación verifica si el usuario ha revisado y aprobado los datos correctos y si la tarjeta ha firmado los datos correctos.

Verificación de la firma de tarjeta.

En la etapa (344), la aplicación verifica si la firma de la tarjeta corresponde con los datos que la aplicación pretendía que la tarjeta firmara. Eso se puede llevar a cabo mediante técnicas tradicionales de verificación de firmas de datos. Por ejemplo, en una realización típica, la firma se obtiene al trocear los datos a firmar y al encriptar la tarjeta el troceado resultante con su clave privada. En dicho caso, la firma se puede verificar al desencriptar la firma con la clave pública que corresponde a la clave privada de la tarjeta y al comparar el resultado desencriptado con un troceado de los datos que se suponen han sido firmados por la tarjeta.

Verificación o recolección de la copia de aplicación del fichero de registro

En la etapa (346), la aplicación verifica o recolecta los contenidos de el/los fichero/s que el lector ha firmado.

En algunas realizaciones, la aplicación ha recuperado del lector los contenidos de los registros firmados y verifica si estos contenidos son coherentes con los eventos y acciones que la aplicación supone han sucedido. Por ejemplo, la aplicación puede verificar si el registro indica si los datos se han presentado al usuario para revisión y aprobación, qué datos se han presentado al usuario y si el usuario ha aprobado o rechazado estos datos. La aplicación también puede, por ejemplo, verificar si la firma de tarjeta que ha obtenido de la tarjeta se ha generado durante la misma sesión de registro segura que la sesión en la que el usuario aprobó los datos. La aplicación puede, por ejemplo,

verificar si la firma de tarjeta se ha registrado en el mismo fichero de registro que los datos aprobados por el usuario. La aplicación puede, por ejemplo, verificar si determinados sellos de tiempo en el fichero de registro están dentro del margen de tolerancia de la aplicación.

En otras realizaciones, la aplicación recolecta una presunta copia de el/los fichero/s de registro que el lector recolectó al registrar en sí mismo todas las acciones y eventos que el lector debía registrar y al aplicar los mismos mecanismos y reglas de registro que se supone el lector aplicaría. Por ejemplo, en una realización típica, el lector puede en un modo de registro seguro registrar todos los comandos de lector y de tarjeta inteligente transparente (y sus correspondientes respuestas) que intercambia con la aplicación, y la aplicación puede registrar de exactamente la misma manera todos los comandos de lector y de tarjeta inteligente transparente que supone se han intercambiado con el lector. Este conjunto de comandos de lector y tarjeta inteligente transparente intercambiados comprende cualquier comando de lector para presentar datos al usuario para revisión y aprobación y cualquier comando de tarjeta inteligente transparente para permitir que la tarjeta genere una firma.

Verificación de la/s firma/s de lector en el/los fichero/s de registro.

En la etapa (348), la aplicación verifica si la firma del lector concuerda con los contenidos del fichero de registro que ha recuperado o recolectado. Eso se puede llevar a cabo mediante técnicas tradicionales de verificación de firmas de datos. Por ejemplo, en una realización típica, la firma se obtiene al trocear los datos a firmar y al encriptar la tarjeta el troceado resultante con su clave privada. En tal caso, la firma se puede verificar al desencriptar la firma con la clave pública que corresponde a la clave privada del lector y comparar el resultado desencriptado con un troceado de los datos (es decir, contenidos de el/los fichero/s de registro) que se supone el lector ha firmado.

Verificar si el usuario ha aprobado los datos correctos.

En la etapa (350), la aplicación verifica si los datos aprobados por el usuario concuerdan con los datos firmados por la tarjeta y/o si los datos aprobados por el usuario concuerdan con los datos de transacción enviados. En algunas realizaciones (p. ej. en realizaciones donde la aplicación recolecta por sí misma una copia de aplicación del fichero de registro), esto puede estar implícito. En otras realizaciones, esta etapa puede ser explícita (p. ej. en realizaciones donde la aplicación recupera los contenidos del fichero de registro, la aplicación puede verificar si los datos que han sido aprobados por el usuario tal y como se grabaron en el fichero de registro se corresponden con los datos que la aplicación pretendía que el usuario revisara y aprobara).

Verificación de si los contenidos del fichero de registro firmado son coherentes con los datos de transacción.

La aplicación puede verificar si los datos de transacción enviados son coherentes con los datos que, según el fichero de registro, han sido revisados y aprobados por el usuario y/o si los datos de transacción enviados y/o estos datos revisados y aprobados son coherentes con los datos firmados por la tarjeta.

En algunas realizaciones, la aplicación puede verificar si determinados sellos de tiempo en el fichero de registro son coherentes con la temporización de determinados eventos de transacción.

Generar señal de confirmación de aprobación del usuario.

En la etapa (352), al completar de manera exitosa las verificaciones anteriores, la aplicación puede generar una señal que confirme que el usuario aprobó la transacción; de lo contrario, la aplicación puede generar una señal que indique que la verificación falló.

Ejecutar transacción.

En la etapa (354), la aplicación puede actuar sobre esta señal de confirmación ejecutando la transacción.

En algunas realizaciones, si cualquiera de las verificaciones anteriores falla, la aplicación puede abortar o cancelar la transacción.

Orden de las etapas del método.

A pesar de que las etapas del método se han descrito anteriormente en un orden en el que estas etapas deben de realizarse en una realización típica, en otras realizaciones algunas etapas se pueden realizar en otro orden, algunas etapas se pueden omitir, se pueden agregar etapas adicionales, algunas etapas se pueden combinar con otras etapas, y algunas etapas pueden comprender subetapas que se pueden interconectar con subetapas de otras etapas.

Por ejemplo, en muchas realizaciones, la aplicación puede intercambiar comandos de tarjeta inteligente en diversos momentos: antes y después de que el lector entre en el modo de registro seguro, antes y después de que el lector deba presentar datos para revisión y aprobación al usuario, antes y después de que la tarjeta deba firmar datos,... Por ejemplo, la aplicación puede intercambiar una serie de comandos de tarjeta inteligente con la tarjeta inteligente antes de entrar en el modo de registro seguro con el fin de determinar el tipo de tarjeta y leer los certificados de clave pública de la tarjeta (p. ej. determinar la identidad del usuario) y establecer los parámetros de configuración de

registro del lector en base a la información así obtenida (p. ej. para indicar qué comandos de tarjeta inteligente transparente se deben registrar, cuál puede ser una función del tipo de tarjeta inteligente).

Mientras que en una realización típica, la etapa en que el lector presenta datos al usuario para revisión y aprobación sucede antes de la etapa en que la tarjeta firma datos, en algunas realizaciones los datos pueden ya haber sido enviados a la tarjeta para su firma antes de que al usuario se le solicite que apruebe los datos.

En algunas realizaciones, la etapa de hacer que el lector entre en modo de registro seguro puede coincidir con la etapa de enviar al lector los datos a revisar y aprobar por el usuario. Por ejemplo, en algunas realizaciones, el lector entra automáticamente en modo de registro seguro cuando recibe un comando de lector para presentar datos a firmar y aprobar por el usuario.

Ventajas de la invención

En una realización típica, el lector y la aplicación están dispuestos de manera tal que se garantiza que el lector registrará tanto los datos aprobados por el usuario como los datos firmados por la tarjeta. El lector y la aplicación pueden, en una realización típica, también estar dispuestos de manera tal que se garantice que el lector registrará cualquier dato que la aplicación envíe durante la sesión de registro seguro al lector para que el usuario lo revise y apruebe y registrará cualquier dato que se envíe durante la sesión de registro seguro a la tarjeta para su firma.

Por ejemplo, en algunas realizaciones, el lector puede registrar todos los comandos de lector que se pueden utilizar para instruir al lector para que presente datos a un usuario y el lector también puede registrar un amplio conjunto de comandos de tarjeta inteligente transparente (por ejemplo, todos los comandos de tarjeta inteligente transparente) con el fin de asegurar que el lector, cuando se encuentra en modo de registro seguro, registrará cualquier dato enviado al lector para su presentación al usuario y cualquier dato presentado a la tarjeta para su firma. En algunas realizaciones, la aplicación puede configurar las reglas de registro del lector y el lector siempre registrará también las reglas de registro, y la aplicación configura las reglas de registro de manera que el lector registrará cualquier comando de lector que se pueda utilizar para instruir al lector para que presente datos a un usuario y cualquier comando de tarjeta inteligente transparente que se pueda utilizar para enviar datos a la tarjeta para su firma.

En tales realizaciones típicas, la aplicación puede obtener pruebas criptográficas que conecten los datos que el usuario aprobó en un lector seguro con los datos que la tarjeta firmó. Más específicamente, al verificar la firma de tarjeta, la aplicación puede verificar qué datos fueron firmados realmente por la tarjeta; al verificar la firma de lector sobre el registro, la aplicación puede además verificar qué datos se revisaron y aprobaron realmente por el usuario (y la aplicación puede, por supuesto, también verificar el hecho de que los datos efectivamente se revisaron y aprobaron); y al verificar los contenidos del registro y la firma de lector sobre el registro, la aplicación puede verificar que la aprobación de datos y la firma de datos tuvo lugar en la misma sesión de registro seguro utilizando el mismo lector y que ningún otro dato se aprobó y/o firmó en esa misma sesión; y la aplicación puede verificar que los datos que el usuario aprobó concuerdan con los datos que se firmaron, comparando los datos que, según el registro, fueron aprobados por el usuario con los datos que, según el registro, fueron firmados por la tarjeta.

De esta manera, la invención resuelve el problema de seguridad de la técnica anterior mediante la cual no se puede excluir que los datos que corresponden a una firma de tarjeta no corresponden con los datos que se han aprobado por el usuario, p. ej. en el visualizador de un PC no seguro. Además, esta solución se puede lograr mediante un lector según la invención que no requiere tener ningún conocimiento acerca del conjunto de comandos de tarjeta inteligente de cualquier tarjeta inteligente específica, de manera que el firmware del lector no necesita saber, interpretar o construir determinados comandos de tarjeta inteligente para firmar datos. Eso tiene la ventaja de que, por un lado, el lector se puede utilizar con una amplia variedad de tarjetas (que presentan conjuntos de comandos muy diferentes) y no necesitan ninguna actualización de firmware si se utilizara un nuevo tipo de tarjeta, mientras que al mismo tiempo, el firmware de lector puede mantenerse relativamente simple con respecto al manejo de los comandos de tarjeta inteligente.

En general, en los párrafos anteriores, los términos "comandos" (como en el caso de "comandos de tarjeta" o "comandos de lector") se pueden entender, a menos que se especifique lo contrario o a menos que quede claro por el contexto, como que comprenden ya sea solo los comandos mismos en un sentido estricto o tanto los comandos mismos como las correspondientes respuestas.

En general, en los párrafos anteriores, los términos "agregar datos a un fichero de registro" se pueden entender, a menos que se especifique lo contrario o a menos que quede claro por el contexto, tanto como agregar los datos al fichero de registro tal y como están o datos representativos de estos datos (tal y como datos que comprenden esos datos o un troceado de esos datos).

Específicamente, cuando se utilizan los términos "registrar un comando de tarjeta" o "registrar un comando de lector" entonces se puede entender, a menos que se especifique lo contrario o a menos que quede claro por el contexto, como que comprenden registrar el par comando-respuesta o datos representativos de la carga útil del par comando-respuesta, es decir, el comando real y la correspondiente respuesta a dicho comando o datos representativos de sus respectivas cargas útiles. Por ejemplo, en algunas realizaciones, algunas partes del comando o de las respuesta, tal

y como valores triviales ya que determinados bytes de la cabecera de comando de códigos de estados de respuesta se pueden omitir cuando se registran los pares comando-respuesta. Además, en algunas realizaciones, para algunos pares comando-respuesta solo se registra la carga útil de comando o solo la carga útil de respuesta.

Los sistemas y dispositivos mencionados han sido descritos con respecto a la interacción entre diversos componentes. Se puede apreciar que dichos sistemas y componentes pueden incluir aquellos componentes o subcomponentes especificados, algunos de los componentes o subcomponentes especificados, y/o componentes adicionales, y según diversos reemplazos y combinaciones de lo anterior. Los subcomponentes también se pueden implementar como componentes acoplados de forma comunicativa a otros componentes en vez de dentro de componentes matriz (jerárquico). Además, se ha de observar que uno o más componentes pueden estar combinados en un único componente lo que ofrece una funcionalidad agregada o divididos en diversos subcomponentes separados, y se pueden proveer una o más capas medias cualquieras, tal y como una capa de gestión, para acoplarse de forma comunicativa a dichos subcomponentes, con el fin de ofrecer una funcionalidad integrada. Cualquier componente descrito aquí también puede interactuar con uno o más componentes que no esté específicamente descrito en la presente memoria, pero que es generalmente conocido por los expertos en la técnica.

Se han descrito una cantidad de implementaciones. Sin embargo, se ha de comprender que se pueden realizar diversas modificaciones. Por ejemplo, se pueden combinar, eliminar, modificar o complementar elementos de una o más implementaciones para formar implementaciones adicionales. Como incluso otro ejemplo, los flujos de lógica representados en las figuras no requieren llevar el orden particular que se muestra, o secuencial, para lograr resultados deseables. Además, se pueden ofrecer otras etapas, o se pueden eliminar etapas, a partir de los flujos descritos, y se pueden agregar otros componentes, o eliminarlos, de los sistemas descritos. Por ejemplo, los módulos o componentes no necesitan realizar todas, o cualquiera, de las funcionalidades atribuidas a dicho módulo en las implementaciones descritas anteriormente, y todas o parte de las funcionalidades atribuidas a un módulo o componente se puede realizar por otro módulo o componente, otro módulo o componente adicional, o directamente no realizarse. De manera acorde, otras implementaciones están comprendidas dentro del alcance de las reivindicaciones adjuntas.

Además, a pesar de que una característica particular de la presente invención se puede haber descrito con respecto a solo una de diversas implementaciones, dicha característica se puede combinar con una o más características distintas de las otras implementaciones, como puede ser deseable o ventajoso para cualquier aplicación determinada o particular. Además, en la medida que se utilicen los términos "incluye", "incluir", "presenta", "contiene" y variantes de los mismos, y otras palabras similares ya sea en la descripción detallada o en las reivindicaciones, esos términos están concebidos para ser inclusivos, de forma similar al término "comprender" como una palabra de transición abierta sin excluir ningún elemento adicional o distinto.

A pesar de que se han descrito diversas realizaciones de la presente invención anteriormente, se ha de comprender que se han presentado sólo a modo de ejemplo y sin limitaciones. En particular, no es posible, por supuesto, describir cada combinación de componentes o metodologías concebibles a los fines de describir la materia reivindicada, pero una persona con experiencia ordinaria en la técnica puede reconocer que son posibles muchas combinaciones y reemplazos adicionales de la presente invención. Por lo tanto, la amplitud y el alcance de la presente invención no se ha de limitar por cualquiera de las realizaciones de ejemplo descritas anteriormente, pero sólo deben definirse según las siguientes reivindicaciones y sus equivalentes.

REIVINDICACIONES

1. Un lector (100) de tarjeta inteligente para generar firmas electrónicas en conjunto con una tarjeta inteligente (98) insertada que comprende:

una interfaz de comunicación (110) para comunicarse con un ordenador anfitrión (99);

un conector (130) de tarjeta inteligente para comunicarse con la tarjeta inteligente;

un primer componente de memoria (140) para almacenar de forma segura una o más claves criptográficas;

una interfaz de usuario que comprende una interfaz de salida del usuario (151) para presentar información al usuario y una interfaz de entrada del usuario (152) para recibir indicaciones del usuario;

un componente de procesamiento de datos (160) para comunicarse con el ordenador anfitrión, comunicarse con la tarjeta inteligente, y controlar la interfaz de usuario;

estando dicho lector de tarjeta inteligente adaptado para intercambiar comandos de tarjeta inteligente con una tarjeta inteligente que utiliza el conector de tarjeta inteligente;

dicho lector de tarjeta inteligente está además adaptado para admitir uno o más comandos de lector para que instruyan al lector para presentar datos a un usuario para su revisión y aprobación por parte del usuario; y para presentar al usuario los datos para revisión y aprobación utilizando la interfaz de salida; y para capturar la aprobación o rechazo del usuario de los datos para revisión o aprobación utilizando la interfaz de entrada;

caracterizado por que dicho lector de tarjeta inteligente además comprende un segundo componente de memoria (140) que tiene un fichero de registro almacenado ahí mismo;

por que dicho lector de tarjeta inteligente está además adaptado para funcionar en un modo de registro seguro en el que el lector de tarjeta inteligente registra en dicho fichero de registro eventos relacionados con la seguridad respecto del lector o del uso del lector;

por que dicho lector de tarjeta inteligente está además adaptado para registrar en dicho fichero de registro los datos pare revisión y aprobación;

y por que dicho lector de tarjeta inteligente está además adaptado para generar una firma de lector en dicho fichero de registro que utiliza al menos una o más de las claves criptográficas almacenadas en dicha primera memoria.

2. El lector de tarjeta inteligente de la reivindicación 1 está además adaptado para registrar en dicho fichero de registro al menos algunos comandos de tarjeta inteligente transparente intercambiados entre el anfitrión y la tarjeta inteligente.

3. El lector de tarjeta inteligente de la reivindicación 2, en donde los comandos de tarjeta inteligente transparente que el lector registra, comprenden comandos de tarjeta inteligente transparente para enviar a la tarjeta inteligente insertada datos a firmar por la tarjeta inteligente o para obtener de la tarjeta inteligente insertada una firma de tarjeta electrónica generada sobre datos enviados.

4. El lector de tarjeta inteligente de la reivindicación 2, en donde el lector está adaptado para registrar todos los comandos de tarjeta inteligente transparente en un período desde un primer punto en el tiempo a un segundo punto en el tiempo.

5. El lector de tarjeta inteligente de la reivindicación 4, en donde el período en el que el lector registra todos los comandos de tarjeta inteligente transparente comprende el período en el que los datos a firmar se envían a la tarjeta inteligente insertada o el período en el que la firma de tarjeta electrónica generada sobre los datos enviados se obtiene de la tarjeta inteligente insertada.

6. El lector de tarjeta inteligente de las reivindicaciones 1 a 5, en donde el lector de tarjeta inteligente almacena un conjunto de datos de configuración que determinan al menos en parte qué eventos registra el lector.

7. El lector de tarjeta inteligente de la reivindicación 6, en donde el lector está adaptado para registrar el conjunto actual de datos de configuración.

8. El lector de tarjeta inteligente de cualquiera de las reivindicaciones 1 a 7 que además comprende un reloj (180) y adaptado para agregar un sello de tiempo a al menos algunos de los eventos registrados.

9. Un método (300a, 300b) para generar una firma electrónica sobre datos a firmar que comprende las etapas de:

conectar (304) un lector (100) de tarjeta inteligente a un ordenador anfitrión (99);

insertar (312) una tarjeta inteligente (98) en el lector;

que el lector entra (320) en modo de registro seguro;

enviar (331) al lector datos para que un usuario revise y apruebe;

presentar (332) al usuario, través del lector utilizando una interfaz de salida del usuario en el lector, los datos para que un usuario revise y apruebe;

capturar (332) a través del lector utilizando una interfaz de entrada del usuario en el lector, la aprobación del usuario de los datos presentados;

registrar (333) mediante el lector en un fichero de registro en el lector los datos para su revisión y aprobación;

enviar (334) a la tarjeta inteligente insertada datos para firmar, generar (334) a continuación a través de la tarjeta inteligente insertada una firma de tarjeta electrónica sobre los datos a firmar enviados, y a continuación obtener (338) de la tarjeta inteligente insertada la firma de tarjeta electrónica generada sobre los datos enviados;

generar (340) a través del lector una firma de lector electrónico sobre el fichero de registro en el lector utilizando un algoritmo de firma de datos criptográficos parametrizados con una clave criptográfica almacenada en el lector, y a continuación obtener (342) la firma de lector electrónico sobre el fichero de registro generado por el lector.

10. El método de la reivindicación 9 comprende además la etapa de registrar (336) a través del lector en el fichero de registro sobre el lector los datos a firmar enviados a la tarjeta o la firma de tarjeta electrónica generada por la tarjeta inteligente insertada.

11. El método de la reivindicación 10, en donde enviar a la tarjeta inteligente insertada datos a firmar y obtener de la tarjeta inteligente insertada la firma de tarjeta electrónica generada sobre los datos enviados, comprende que el ordenador anfitrión intercambie (328) comandos de tarjeta inteligente transparente con la tarjeta inteligente insertada utilizando el lector de tarjeta inteligente; y en donde registrar a través del lector en el fichero de registro sobre el lector, los datos a firmar enviados a la tarjeta o a la firma de tarjeta electrónica generada por la tarjeta inteligente insertada comprende registrar a través del lector en el fichero de registro sobre el lector al menos algunos de los comandos de tarjeta inteligente transparente intercambiada.

12. El método de la reivindicación 11, en donde los comandos de tarjeta inteligente transparente que el ordenador anfitrión intercambia con la tarjeta inteligente insertada utilizando el lector de tarjeta inteligente comprende al menos comandos de tarjeta inteligente transparente para enviar a la tarjeta inteligente insertada datos a firmar; y en donde al menos algunos de los comandos de tarjeta inteligente transparente intercambiados que el lector registra en el registro sobre el lector comprenden al menos comandos de tarjeta inteligente transparente para enviar a la tarjeta inteligente insertada datos a firmar o comandos de tarjeta inteligente transparente para obtener de la tarjeta inteligente insertada una firma de tarjeta electrónica generada sobre datos enviados.

13. El método de la reivindicación 10 o reivindicación 12, en donde al menos alguno de los comandos de tarjeta inteligente transparente que el lector registra en el fichero de registro sobre el lector comprende todos los comandos de tarjeta inteligente transparente intercambiados durante un período determinado, en donde el período en donde el lector registra todos los comandos de tarjeta inteligente transparente intercambiados comprende el período en donde los datos a firmar se envían a la tarjeta inteligente insertada o el período en donde la firma de tarjeta electrónica generada sobre los datos enviados se obtiene de la tarjeta inteligente insertada.

14. El método de cualquiera de las reivindicaciones 9 a 13 además comprende configurar un conjunto de datos de configuración sobre el lector que determina al menos parcialmente qué eventos registra el lector en el fichero de registro sobre el lector.

15. El método de la reivindicación 14 comprende además configurar el conjunto de datos de configuración de manera que el lector registre en un fichero de registro sobre el lector los datos para revisión y aprobación.

16. El método de la reivindicación 14 o reivindicación 15 además comprende configurar el conjunto de datos de configuración, de manera que el lector registre en un fichero de registro sobre el lector un conjunto de comandos de tarjeta inteligente transparente que comprende comandos de tarjeta inteligente para enviar a la tarjeta inteligente insertada datos a firmar o para obtener de la tarjeta inteligente insertada una firma electrónica generada sobre datos enviados a la tarjeta inteligente.

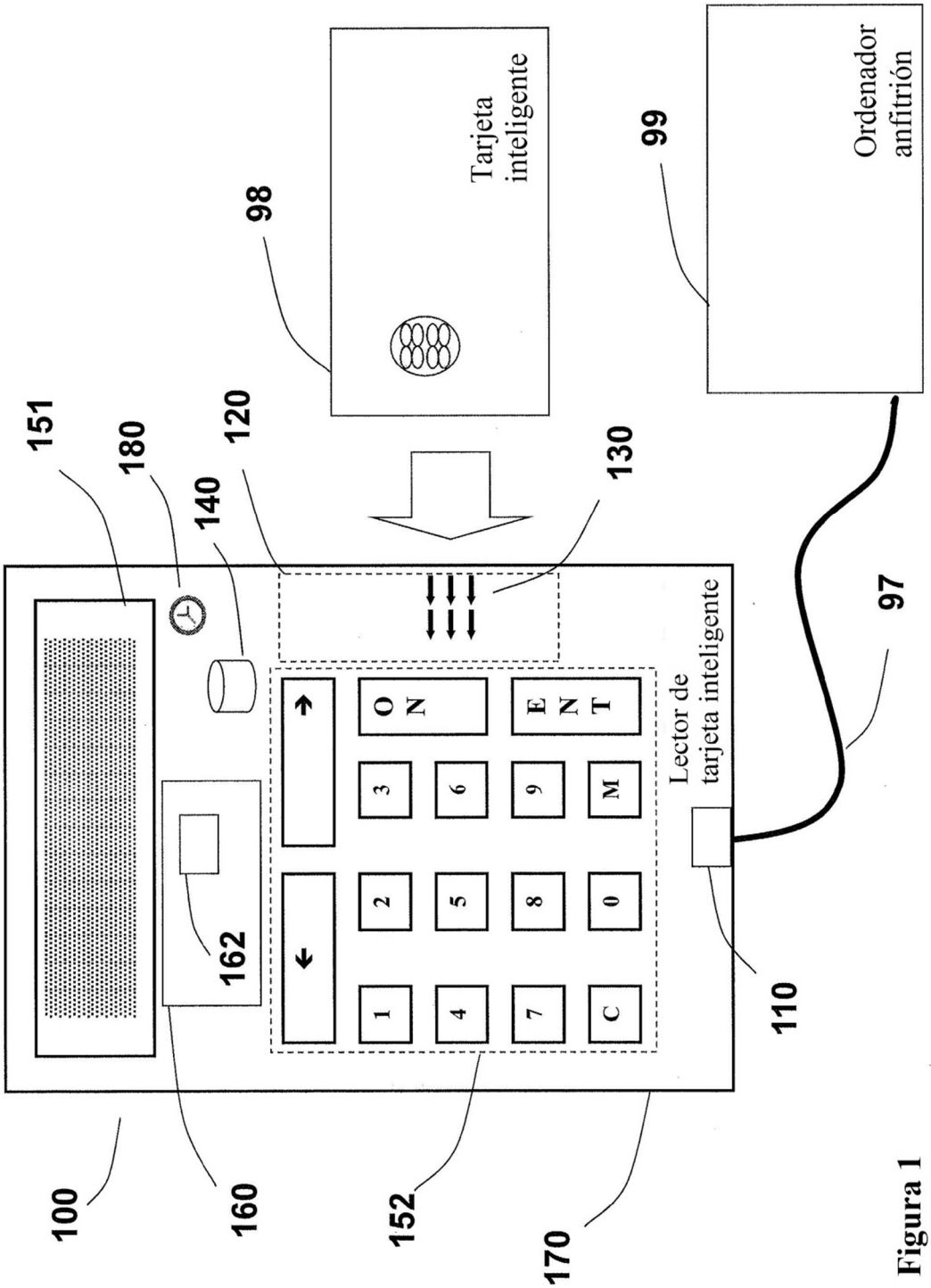
Tarjeta inteligente
Ordenador anfitrión
98
99
151
180
140
120
130
97
Lector de tarjeta inteligente
ON
ENT
1
2
3
4
5
6
7
8
9
0
C
M
162
110
100
160
152
170

Figura 1

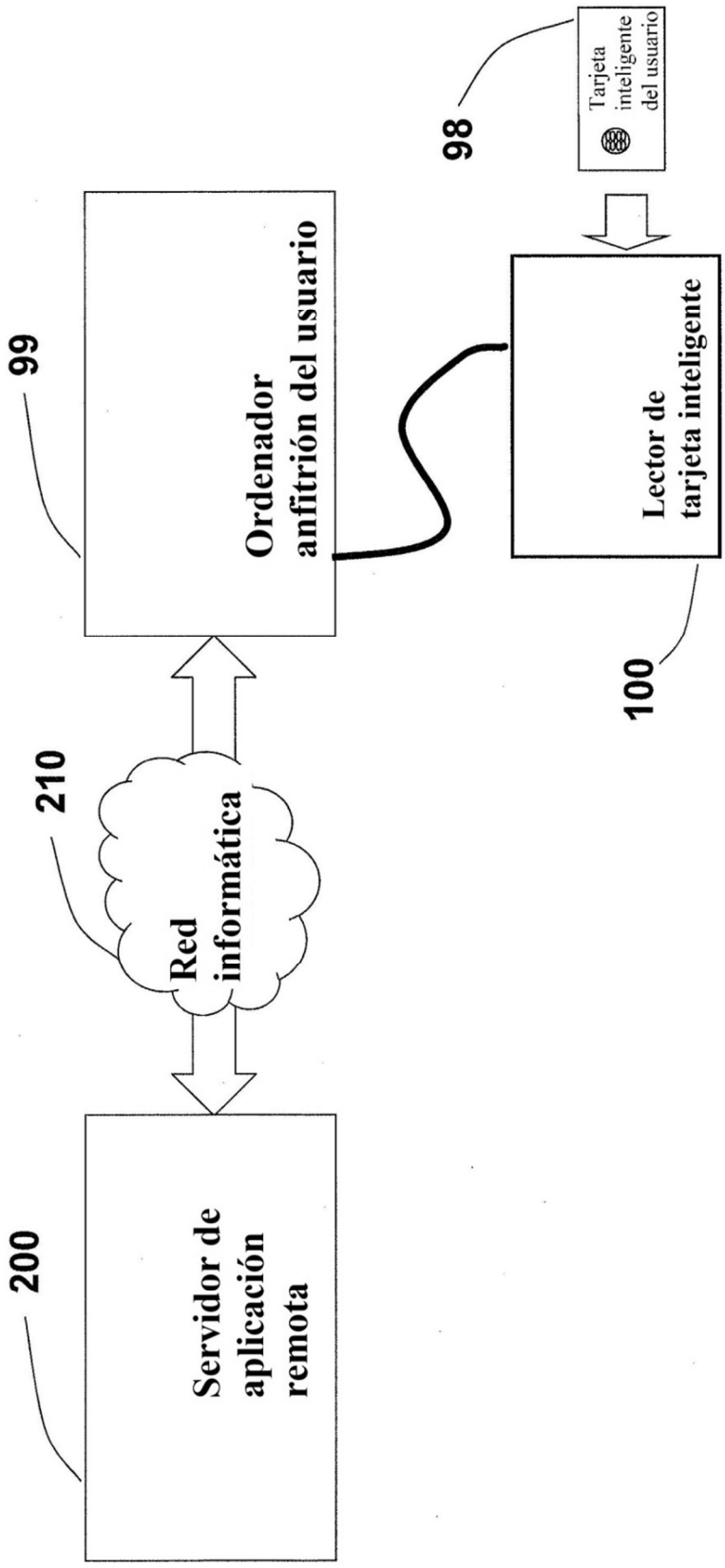
98
Tarjeta inteligente del usuario
99
Ordenador anfitrión del usuario
Lector de tarjeta inteligente
100
210
Red informática
200
Servidor de aplicación remota

Figura 2

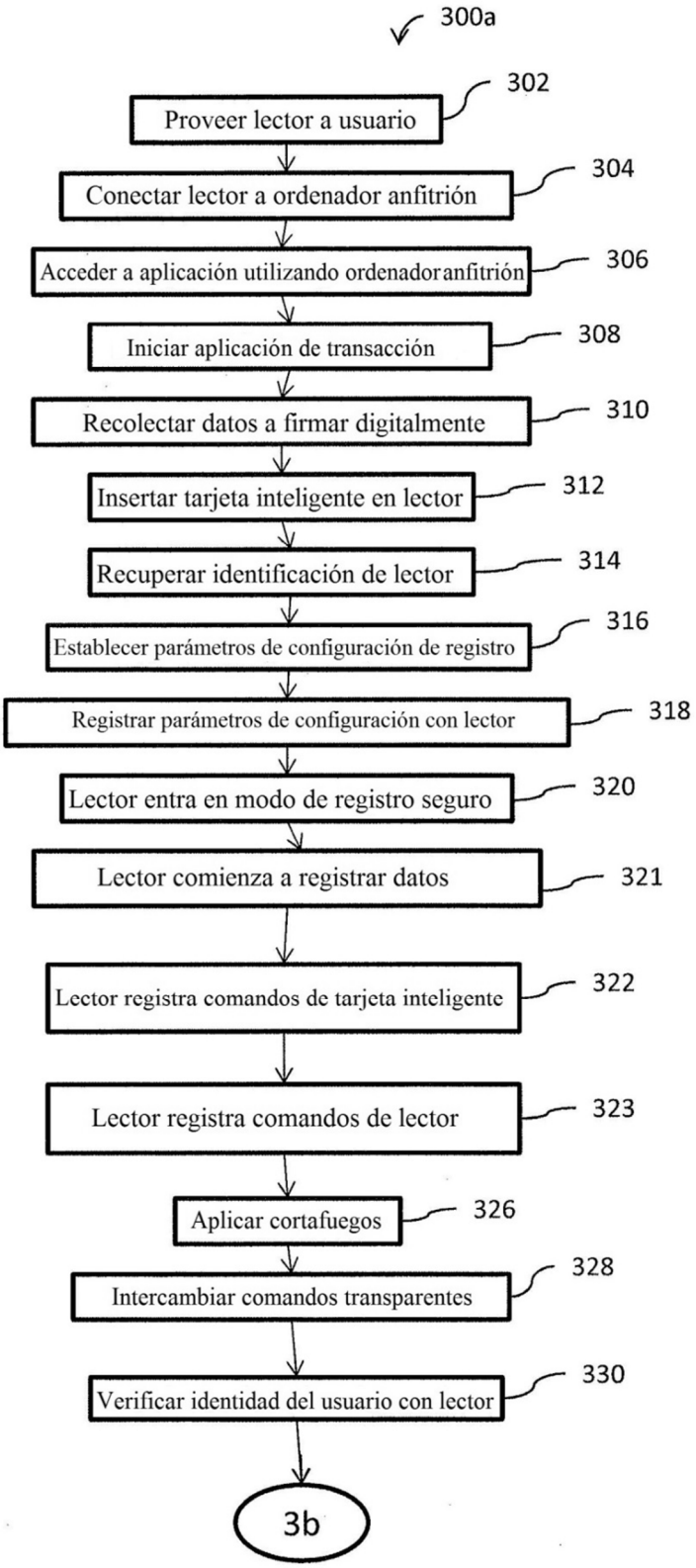
300a
302
Proveer lector a usuario
304
Conectar lector a ordenador anfitrión
306
Acceder a aplicación utilizando ordenador anfitrión
308
Iniciar aplicación de transacción
310
Recolectar datos a firmar digitalmente
312
Insertar tarjeta inteligente en lector
314
Recuperar identificación de lector
316
Establecer parámetros de configuración de registro
318
Registrar parámetros de configuración con lector
320
Lector entra en modo de registro seguro
321
Lector comienza a registrar datos
322
Lector registra comandos de tarjeta inteligente
323
Lector registra comandos de lector
326
Aplicar cortafuegos
328
Intercambiar comandos transparentes
330
Verificar identidad del usuario con lector
3b

FIG. 3a

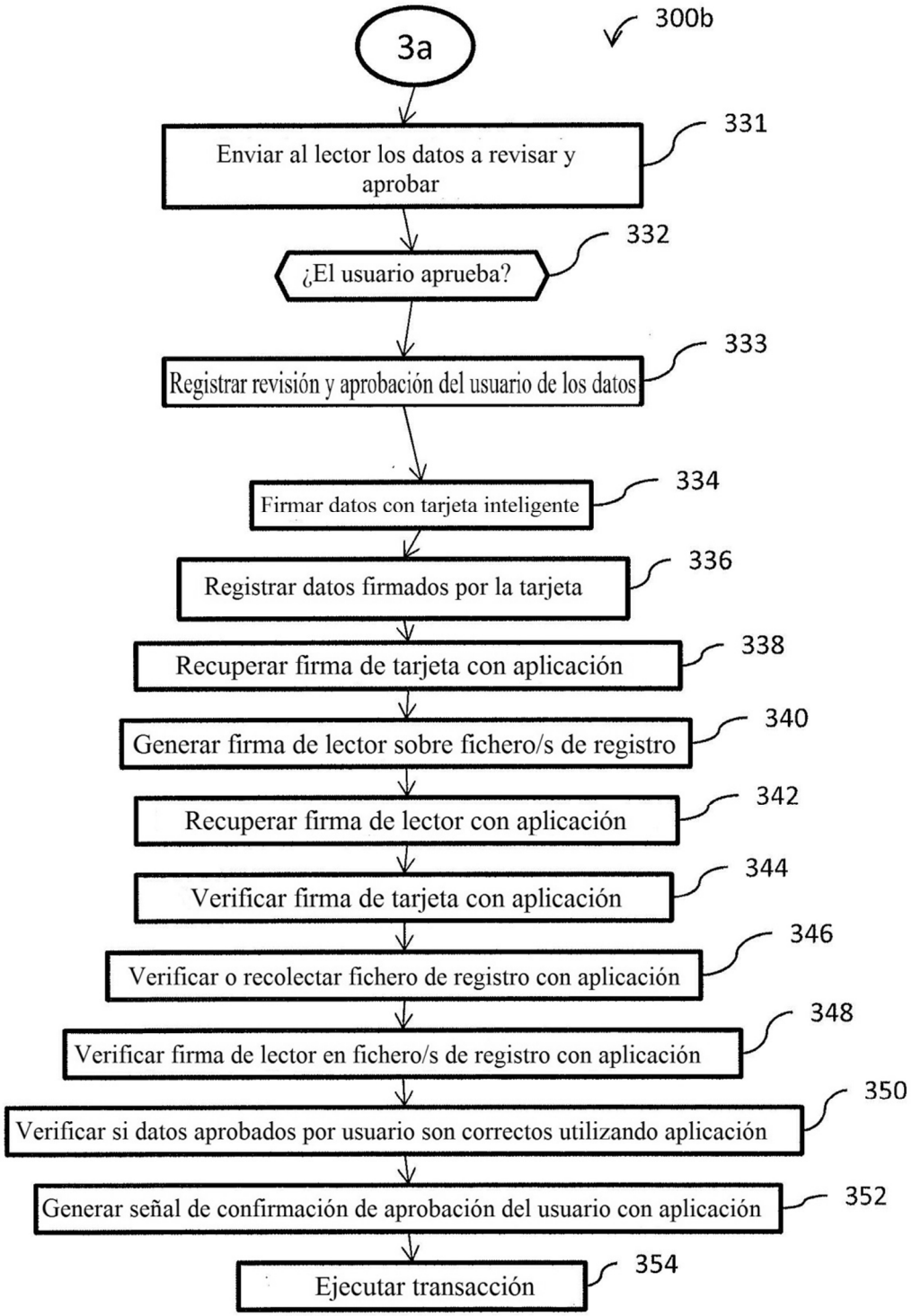
300b
3a
Enviar al lector los datos a revisar y aprobar
331
¿El usuario aprueba?
332
Registrar revisión y aprobación del usuario de los datos
333
Firmar datos con tarjeta inteligente
334
Registrar datos firmados por la tarjeta
336
Recuperar firma de tarjeta con aplicación
338
Generar firma de lector sobre fichero/s de registro
340
Recuperar firma de lector con aplicación
342
Verificar firma de tarjeta con aplicación
344
Verificar o recolectar fichero de registro con aplicación
346
Verificar firma de lector en fichero/s de registro con aplicación
348
Verificar si datos aprobados por usuario son correctos utilizando aplicación
350
Generar señal de confirmación de aprobación del usuario con aplicación
352
Ejecutar transacción
354

FIG. 3b