(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 374 932**

(51) Int. CI.:
G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06119047 .6**
(96) Fecha de presentación: **16.08.2006**
(97) Número de publicación de la solicitud: **1890246**
(97) Fecha de publicación de la solicitud: **20.02.2008**

(54) Título: **HABILITACIÓN DEL USO DE UN CERTIFICADO ALMACENADO EN UNA TARJETA INTELIGENTE.**

(45) Fecha de publicación de la mención BOPI:
23.02.2012

(45) Fecha de la publicación del folleto de la patente:
23.02.2012

(73) Titular/es:
RESEARCH IN MOTION LIMITED
295 Phillip Street
Waterloo, Ontario N2L 3W8 , CA

(72) Inventor/es:
Brown, Michael K;
Adams, Neil y
Little, Herb

(74) Agente: **de Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Habilitación del uso de un certificado almacenado en una tarjeta inteligente.

Las tarjetas inteligentes (SC –"Smart Cards") se utilizan de forma generalizada en combinación con medidas de seguridad tales como la autentificación y la encriptación o cifrado. Por ejemplo, a fin de acceder a un dispositivo computerizado y acceder a información utilizando el dispositivo computerizado, puede ser necesario acoplar una tarjeta inteligente al dispositivo computerizado. El acceso al dispositivo computerizado y a la información puede ser concedido a continuación de una interacción satisfactoria entre el dispositivo computerizado y la tarjeta inteligente. La interacción puede implicar una introducción por parte del usuario.

Una tarjeta inteligente puede haberse programado o de otro modo ajustado para tener información relativa a la seguridad. Un ejemplo de ello es la información de identificación de la propia tarjeta inteligente, por ejemplo, un número de serie. Otro ejemplo es una palabra de paso para autentificación, de tal manera que el acceso a la capacidad funcional de la tarjeta inteligente puede requerir el conocimiento de la palabra de paso para autentificación. Un ejemplo adicional lo constituyen uno o más archivos que incluyen elementos de información específicos, tales como información de identificación personal de uno o más usuarios autorizados de la tarjeta inteligente.

Aún otro ejemplo es un par de certificado / clave privada. Un certificado puede incluir una clave pública que está asociada con la clave privada del par, y puede también incluir una firma, información de identidad y un campo que define uno o más propósitos asignados al certificado. Las claves privadas están almacenadas en un área segura de la tarjeta inteligente y no son accesibles desde el exterior. Los certificados, por otra parte, pueden ser exportados desde la tarjeta inteligente a otros dispositivos.

Un certificado puede ser asignado, por ejemplo, para la autentificación de un usuario, para el cifrado de información, para firmar información, para asegurar la exploración de web, para el registro de entrada en un servicio de WEB y/o para proporcionar un acceso a una red o a un dispositivo. Una tarjeta inteligente puede incluir uno o más pares de certificado / clave privada.

Un certificado que ha sido asignado a un propósito particular puede incluir información específica del propósito. Por ejemplo, un certificado asignado para el registro de entrada en una red puede incluir información acerca de la red. El propósito definido en un certificado no es obligatorio, y un certificado puede ser utilizado para cualquier otro propósito.

La información se inicializa o introduce por primera vez, por lo común, en una tarjeta inteligente utilizando un equipo de uso exclusivo o dedicado y, habitualmente, por personal dedicado o especializado, tal como miembros de un departamento de IT (Tecnología de Información –"Information Technology") de una organización. Una tarjeta inteligente puede ser inicializada para propósitos específicos con un número particular de pares de certificado / clave privada que se asignan para estos propósitos específicos. En un momento posterior, sin embargo, puede existir la necesidad de utilizar la tarjeta inteligente para un propósito que no se ha definido en ninguno de los certificados. Puede requerirse entonces la intervención del personal especializado con el fin de inicializar un par adicional de certificado / clave privada contenido en la tarjeta inteligente.

El documento US 5.721.781 divulga un sistema de autentificación que incluye un dispositivo de información portátil, tal como una tarjeta inteligente, que está configurado para almacenar y procesar o tratar múltiples aplicaciones diferentes. A la tarjeta inteligente se le asigna su propio certificado digital, que contiene una firma digital procedente de una autoridad de certificación de confianza y una clave pública única o exclusiva. A cada una de las aplicaciones almacenadas en la tarjeta inteligente se le asigna también un certificado asociado que tiene la firma digital de la autoridad de certificación. El sistema incluye, de manera adicional, un terminal que es capaz de acceder a la tarjeta inteligente. El terminal tiene al menos una aplicación compatible que funciona en combinación con una aplicación existente en la tarjeta inteligente. Al terminal se le asigna su propio certificado, que también contiene la firma digital procedente de la autoridad de certificación de confianza y una clave pública exclusiva. De forma similar, a la aplicación existente en el terminal se le da un certificado digital asociado. Durante una sección de transacción, la tarjeta inteligente y el terminal intercambian sus certificados para autentificarse mutuamente. Tras ello, se selecciona una aplicación de tarjeta inteligente, y los certificados relacionados tanto para la aplicación de tarjeta inteligente como para la aplicación de terminal son intercambiados entre la tarjeta inteligente y el terminal con el fin de autentificar las aplicaciones. Adicionalmente, el tenedor de la tarjeta introduce un PIN [Número de Identificación Personal –"Personal Identification Number"] único o exclusivo en el terminal. El PIN se hace pasar a la tarjeta inteligente para utilizarse en la autentificación del tenedor de la tarjeta. El sistema de autentificación en tres niveles o escalones favorece la seguridad en las transacciones con tarjeta inteligente.

GENERALIDADES

Una tarjeta inteligente es inicializada, típicamente, con contenido utilizando un equipo de uso exclusivo o dedicado y personal especializado, tal como miembros de un departamento de IT de una organización. Una tarjeta inteligente

puede ser inicializada con uno o más pares constituidos por un certificado y una clave privada, y uno cualquiera de los certificados puede ser asignado con uno o dos propósitos particulares. Los propósitos pueden estar incluidos en el certificado.

Un problema que debe resolverse es que, si una tarjeta inteligente se ha de utilizar para un propósito particular y no hay ningún certificado inicializado en la tarjeta inteligente para este propósito, se necesita, típicamente, una operación bastante compleja para inicializar dicho certificado en la tarjeta inteligente. Otro problema es que, incluso aunque se haya inicializado un certificado en la tarjeta inteligente para este propósito, si un dispositivo computerizado que ha de utilizar el certificado ha sido actualizado o renovado, es posible que la información acerca del certificado haya sido borrada del dispositivo computerizado.

De acuerdo con ello, se proporciona un método según se detalla en la reivindicación 1. Características ventajosas se proporcionan en las reivindicaciones dependientes. Se proporciona un dispositivo según se detallada en la reivindicación 10. El usuario/a puede necesitar identificarse a sí mismo/a mediante la introducción de una o más palabras de paso correctas, y será instado entonces a seleccionar un certificado. El dispositivo puede importar el certificado seleccionado desde la tarjeta inteligente.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Realizaciones proporcionadas a modo de ejemplo y no como limitación se ilustran en las figuras de los dibujos que se acompañan, en los que los mismos números de referencia indican elementos correspondientes, análogos o similares, y en los cuales:

La Figura 1 es un diagrama esquemático de un sistema proporcionado a modo de ejemplo, que comprende una tarjeta inteligente, un lector de tarjeta inteligente y dispositivos computerizados;
La Figura 2 es un diagrama de bloques de un dispositivo computerizado proporcionado a modo de ejemplo;
La Figura 3 es un diagrama de bloques de un lector de tarjeta inteligente proporcionado a modo de ejemplo;
La Figura 4 es un diagrama de bloques de una tarjeta inteligente proporcionada a modo de ejemplo;
La Figura 5 es un diagrama de flujo de un método proporcionado a modo de ejemplo para habilitar el uso de un certificado almacenado en una tarjeta inteligente; y
La Figura 6 es un diagrama de flujo de otro método proporcionado a modo de ejemplo para habilitar el uso de un certificado almacenado en una tarjeta inteligente.

Se apreciará que, por simplicidad y claridad de ilustración, los elementos mostrados en las figuras no han sido necesariamente dibujados a escala. Por ejemplo, las dimensiones de algunos elementos pueden haberse exagerado con respecto a otros elementos en aras de la claridad.

DESCRIPCIÓN DE LAS REALIZACIONES PREFERIDAS

En la siguiente descripción detallada se exponen numerosos detalles específicos con el fin de proporcionar una comprensión profunda de las realizaciones. Sin embargo, se comprenderá por parte de las personas con conocimientos ordinarios de la técnica que las realizaciones pueden ponerse en práctica sin estos detalles específicos. En otros casos, métodos, procedimientos, componentes y circuitos bien conocidos no se han descrito en detalle para no oscurecer las realizaciones.

La Figura 1 es un diagrama esquemático de un sistema 100 proporcionado a modo de ejemplo, que comprende una SC 102, un lector de tarjeta inteligente (SCR –“smart card reader”) 104 y dispositivos computerizados 106 y 108.

Las tarjetas inteligentes son dispositivos de seguridad personalizados, definidos por la norma ISO7816 y sus derivadas, y publicada por la Organización Internacional para la Normalización [ISO –“International Organization for Santardization”]. Una tarjeta inteligente puede tener el mismo factor de forma o geométrico de una tarjeta de crédito y puede incluir un dispositivo semiconductor. El dispositivo semiconductor puede incluir una memoria que puede ser programada con información de seguridad (por ejemplo, una clave de desencriptación o desciframiento privada, una clave de firma privada, parámetros biométricos, un certificado de autentificación, etc.), y puede incluir un motor o máquina de desciframiento, por ejemplo, un procesador y/o lógica dedicada o de uso exclusivo, por ejemplo, lógica de desciframiento dedicada y/o lógica de firma dedicada. Una tarjeta inteligente puede incluir un conectador para alimentar con energía el dispositivo semiconductor y llevar a cabo la comunicación en serie con un dispositivo externo. Una tarjeta inteligente puede ser utilizada para la identificación visual, tarjetas temporales, acceso a puertas y fines similares.

Un SCR es un dispositivo que se comunica tanto con la SC como con un dispositivo computerizado y puede utilizarse, por tanto, para acoplarlos o conectarlos. El SCR puede incluir una o más aplicaciones de accionamiento para comunicarse con la SC y con el dispositivo computerizado.

Algunos lectores de tarjeta inteligente son susceptibles de ser mecánica y eléctricamente acoplados o conectados al dispositivo computerizado. Por ejemplo, algunos lectores de tarjeta inteligente se han diseñado para ser permanentemente instalados dentro de un dispositivo computerizado tal como una computadora de sobremesa.

Otros lectores de tarjeta inteligente, por ejemplo, los que se dan con un factor de forma o geométrico de una tarjeta de PCMCIA (Asociación Internacional de Tarjetas de Memoria de Computadoras Personales –"Personal Computer Memory Card International Association"), se han diseñado para ser fácilmente instalables y extraíbles en un cargador apropiado de un dispositivo computerizado móvil tal como una computadora portátil. Otros lectores de tarjeta inteligente se han diseñado para conectarse a un dispositivo computerizado a través de un cable eléctrico.

Se conocen, sin embargo, los lectores de tarjeta inteligente que están mecánicamente desconectados del dispositivo computerizado y pueden comunicarse con el dispositivo computerizado utilizando comunicación inalámbrica. Puesto que un lector de tarjeta inteligente inalámbrico no requiere de acoplamiento mecánico con el dispositivo computerizado, puede, en principio, mantener sesiones de comunicación en paralelo con dos o más dispositivos computerizados a través de la comunicación inalámbrica.

Si bien la Figura 1 muestra la tarjeta inteligente 102 insertada en el SCR 104, las realizaciones de esta invención son igualmente aplicables a tarjetas inteligentes sin contacto que se comunican con sus lectores de tarjeta inteligente por otros medios, por ejemplo, utilizando tecnología de identificación por radiofrecuencia (RFID –"radio frequency identification").

Las realizaciones de la invención son aplicables a cualquier dispositivo computerizado, ya sea estacionario o móvil, que sea capaz de comunicarse con un SCR. Por ejemplo, la comunicación puede ser posible a través de unos medios con instalación de cables, o cableados, sin cables o inalámbricos, u ópticos.

Una lista no exhaustiva de ejemplos para los dispositivos 106 y 108 incluyen cualquiera de los siguientes dispositivos computerizados, por ejemplo, computadoras de servidor, computadoras de agenda, computadoras portátiles, computadoras móviles, terminales móviles, computadoras de bolsillo, computadoras personales de sobremesa, asistentes personales digitales (PDAs- "personal digital assistants"), computadoras de mano, teléfonos celulares, reproductores de MP3 y dispositivos similares.

En el sistema 100 proporcionado a modo de ejemplo, el dispositivo computerizado 108 es capaz de comunicarse con el SCR 104 y, a través del SCR 104, con la SC 102. Además, el dispositivo computerizado 108 es capaz de comunicarse con el dispositivo computerizado 106.

La Figura 2 es un diagrama de bloques de un dispositivo computerizado 200 proporcionado a modo de ejemplo, de acuerdo con algunas realizaciones de la invención. El dispositivo 200 es un ejemplo de dispositivo 108.

El dispositivo 200 comprende una interfaz de comunicación 202, un procesador 204, conectado a la interfaz de comunicación 202, y una memoria 206, conectada al procesador 204. La memoria 206 puede estar fija en el dispositivo 200 o ser extraíble de este. El procesador 204 y la memoria 206 pueden formar parte del mismo circuito integrado o estar en circuitos integrados independientes.

En el ejemplo que se ha mostrado en la Figura 2, la interfaz de comunicación 202 es una interfaz de comunicación inalámbrica 202 y el dispositivo 200 también comprende una antena 208. La interfaz de comunicación inalámbrica 202 comprende una radio 210, conectada a la antena 208, y un procesador 212, conectado a la radio 210. La interfaz de comunicación inalámbrica 202 y el procesador 204 pueden formar parte del mismo circuito integrado o encontrarse en circuitos integrados independientes.

El dispositivo 108 puede ser capaz de comunicarse con el SCR 104 por medio de una interfaz de comunicación 202, y puede ser capaz de comunicarse con el dispositivo 106 a través de la interfaz de comunicación 202. Alternativamente, o en lugar de ello, el dispositivo 108 puede incluir una interfaz de comunicación 214, y puede ser capaz de comunicarse con el dispositivo 106 a través de la interfaz de comunicación 214.

La memoria 206 almacena un dispositivo de accionamiento 216 de SCR, un dispositivo de autentificación 218, una política de seguridad 220 y una palabra de paso 222 de dispositivo. El dispositivo 200 incluye una interfaz 224 para introducción por parte de una persona, tal como un teclado, y una interfaz de salida 226 para una persona, tal como un dispositivo de presentación visual. Como parte de un procedimiento de autentificación, la interfaz de salida 226 para un usuario puede instar al usuario a introducir una palabra de paso de dispositivo utilizando la interfaz 224 para introducción por un usuario, y el dispositivo de autentificación 218 puede comparar la palabra de paso introducida con la palabra de paso 222 de dispositivo.

La política de seguridad 220 puede haber sido predefinida y/o ser susceptible de descargarse al dispositivo 108 desde el dispositivo 106, y puede definir parámetros y comportamientos relacionados con la seguridad para el dispositivo 108. Por ejemplo, la política de seguridad 220 puede definir si, y para qué propósito, se han de utilizar una palabra de paso para autentificación que se ha almacenado en una tarjeta inteligente y la palabra de paso 222 de dispositivo, y puede definir cualidades de estas palabras de paso. En otros ejemplos, la política de seguridad 220 puede definir si se ha de utilizar o no una autentificación de respuesta a una pregunta de dos factores, si se permiten o no certificados débiles, y cómo tratar certificados revocados, inválidos o en los que no se confía.

La memoria 206 también almacena código ejecutable 230 que, cuando es llevado a efecto o ejecutado por el procesador 204, hace que el dispositivo 200 lleve a cabo su parte en los métodos que se describen más adelante en la presente memoria.

La Figura 3 es un diagrama de bloques de un SCR 300 proporcionado a modo de ejemplo, de acuerdo con algunas realizaciones de la invención. El SCR 300 es un ejemplo de SCR 104.

El SCR 300 incluye una interfaz de comunicación 302, un procesador 304, conectado a la interfaz de comunicación inalámbrica 302, una interfaz 306 de soporte físico o hardware y una memoria 308, conectada al procesador 304. Por ejemplo, la interfaz 306 de hardware es un conectador que coincide con un conectador correspondiente con patas de contacto existente en la tarjeta inteligente. La memoria 308 puede estar encajada o parcialmente encajada dentro del procesador 304. La memoria 308 almacena un dispositivo de accionamiento 310 de lector de tarjeta inteligente y un dispositivo de accionamiento 312 de tarjeta inteligente.

El procesador 304 y la memoria 308 pueden formar parte del mismo circuito integrado o encontrarse en circuitos integrados independientes.

En el ejemplo que se muestra en la Figura 3, la interfaz de comunicación 302 es una interfaz de comunicación inalámbrica 302, y el SCR 300 comprende también una antena 316. La interfaz de comunicación inalámbrica 302 comprende una radio 318, conectada a la antena 316, y un procesador 320, conectado a la radio 318. La interfaz de comunicación inalámbrica 302 y el procesador 304 pueden formar parte del mismo circuito integrado o estar en circuitos integrados independientes.

La Figura 4 es un diagrama de bloques de una SC 400 proporcionada a modo de ejemplo, de acuerdo con algunas realizaciones de la invención. La SC 400 es un ejemplo de SC 102. La SC 400 incluye una interfaz 402 de hardware, un controlador 404, conectado a la interfaz 402 de hardware, y una memoria 406, conectada al controlador 404.

La memoria 406 almacena un dispositivo de accionamiento 408 para manejar la capacidad funcional del SC 400, una identificación 410 de tarjeta inteligente, por ejemplo, un número de serie, y uno o más archivos 412 con información acerca del propietario de la tarjeta inteligente y/o cualquier otra información. La memoria 406 puede almacenar una palabra de paso 414 para autentificación, destinada a ser utilizada en combinación con el dispositivo de autentificación 218 del SCR 300. Como parte de un procedimiento de autentificación, la interfaz de salida 226 para un usuario puede instar al usuario a introducir una palabra de paso para autentificación utilizando la interfaz 224 para introducción por parte del usuario, y el dispositivo de autentificación 218 puede comparar la palabra de paso introducida con la palabra de paso 414 para autentificación.

La memoria 406 puede almacenar uno o más pares 416, cada uno de los cuales comprende una clave privada 418 ($K_{PRIVADA}$) y un certificado 420. Cualquiera de los certificados 420 puede comprender una clave pública ($K_{PÚBLICA}$) 422, asociada con la clave privada 418, y una firma 424, información de identificación 426 y una o más definiciones 428 de propósitos asignados al certificado.

La memoria 406 puede almacenar, además, un PIN (Número de Identificación Personal) 430 de tarjeta inteligente.

Una lista no exhaustiva de ejemplos para las antenas 208 y 316 incluye antenas de dipolo, antenas de monopolo, antenas cerámicas de múltiples capas, antenas en F invertida planas, antenas de bucle o lazo, antenas de proyección o lobulares, antenas duales, antenas omnidireccionales y cualesquiera otras antenas adecuadas.

Una lista no exhaustiva de ejemplos de protocolos de comunicación con los que pueden ser compatibles las interfaces de comunicación 202 y 302, incluye Bluetooth®, ZigBee™, identificación de radiofrecuencia (RFID –"radio frequency identification"), banda ultraancha (UWB –"ultra wideband"), IEEE 802.11, y protocolos de comunicación poseídos en propiedad.

Una lista no exhaustiva de ejemplos para los procesadores 204, 212, 304 y 320, y para el controlador 404, incluye una unidad central de procesamiento (CPU –"central processing unit"), un procesador de señal digital (DSP –"digital signal processor"), una computadora de conjunto de instrucciones reducido (RISC –"reduced instruction set computer"), una computadora de conjunto de instrucciones complejo (CISC –"complex instruction set computer"), y elementos similares. Por otra parte, los procesadores 206, 218, 306 y 318 pueden formar parte de circuitos integrados específicos de aplicación (ASICs –"application specific integrated circuits") o pueden formar parte de productos estándar específicos de aplicación (ASSPs- "application specific standard products").

Una lista no exhaustiva de ejemplos para las memorias 206, 308 y 406 incluye cualquier combinación de los siguientes:

a) dispositivos semiconductores tales como registros, circuitos de retención, memoria de solo lectura (ROM –

"read only memory"), ROM de máscara, dispositivos de memoria de solo lectura programables y borrables eléctricamente (EEPROM –"electrically erasable programmable read only memory"), dispositivos de memoria de tipo flash o de refrescamiento por impulsos, dispositivos de memoria de acceso aleatorio no volátil (NVRAM –"non-volatile random access memory"), dispositivos de memoria de acceso aleatorio, sincrónica y dinámica (SDRAM –"synchronous dynamic random access memory"), dispositivos de memoria de acceso aleatorio dinámica de RAMBUS (RDRAM –"RAMBUS dynamic random access memory"), dispositivos de memoria de doble velocidad de datos (DDR –"double data rate"), memoria de acceso aleatorio estática (SRAM –"static random access memory"), memoria extraíble de bus de serie universal (USB –"universal serial bus"), y dispositivos similares;

b) dispositivos ópticos, tales como memoria de solo lectura de disco compacto (CD ROM –"compact disk read only memory") y dispositivos similares; y

c) dispositivos magnéticos, tales como un disco duro, un disco flexible, una cinta magnética y dispositivos similares.

El dispositivo 200, el SCR 300 y la SC 400 incluyen componentes adicionales que no se han mostrado en las Figuras 2, 3 y 4 y que, en aras de la claridad, no se describen en la presente memoria.

La Figura 5 es un diagrama de flujo de un método proporcionado a modo de ejemplo para habilitar el uso de un certificado almacenado en una tarjeta inteligente 400.

Según se indica por la referencia 500, el dispositivo 200 almacena en la memoria 206 una política de seguridad 220 que requiere un certificado instalado en la SC 400 para un propósito particular. Por ejemplo, la política de seguridad 220 puede requerir un certificado para el propósito de la autentificación de un usuario, una pregunta / respuesta de autentificación de dos factores, el cifrado de información, información de firma, la seguridad de la exploración de web, el registro de entrada en un servicio de WEB y/o la facilitación del acceso a una red o a un dispositivo.

Si el dispositivo 200 no se ha bloqueado todavía, según se indica por la referencia 504, el dispositivo 200 puede quedar bloqueado. Conforme a lo indicado por la referencia 506, un usuario que desea llevar a cabo una operación que implica el dispositivo 200, conecta la SC 400 al SCR 300 y el SCR 300 al dispositivo 200. Según se indica por la referencia 508, el usuario o usuaria inicializa un procedimiento para autentificarse a sí mismo/a frente al dispositivo 200, por ejemplo, encendiendo el dispositivo 200 o activando la interfaz de usuario 224 de una manera predefinida.

Conforme a lo indicado por la referencia 510, el dispositivo 200 puede instar al usuario a establecer una nueva palabra de paso del dispositivo y puede almacenar la palabra de paso del dispositivo recibida como palabra de paso 222 del dispositivo. En caso contrario, si la palabra de paso 222 del dispositivo ya está definida, el dispositivo 200 pude instar al usuario a introducir una palabra de paso de dispositivo y puede comparar la palabra de paso introducida con un valor almacenado en la palabra de paso 222 del dispositivo.

Según se indica por la referencia 512, el dispositivo 200 puede instar al usuario a establecer una nueva palabra de paso de autentificación y puede almacenar la palabra de paso de autentificación recibida como palabra de paso 414 para autentificación en la memoria 406 de la SC 400. En caso contrario, si la palabra de paso 414 para autentificación ya se ha definido, el dispositivo 200 puede instar al usuario a introducir una palabra de paso para autentificación y puede comparar la palabra de paso introducida con un valor almacenado en la palabra de paso para autentificación 414.

Según se indica por la referencia 513, el dispositivo 200 identifica que la SC 400 no almacena un certificado que se ha asignado con el propósito particular requerido por la política de seguridad 220.

De acuerdo con lo indicado por la referencia 514, el dispositivo 200 puede instar al usuario a seleccionar uno de los certificados 420 para el propósito particular definido en la política de seguridad 220. Según se indica en la reivindicación 516, el dispositivo 200 recibe del usuario una selección de uno de los certificados 420. Según la referencia 518, el dispositivo 200 importa el certificado seleccionado de la SC 400.

Conforme a lo indicado por la referencia 520, el dispositivo 200 puede almacenar una copia del certificado seleccionado en un área 232 de almacenamiento de certificado contenida en la memoria 206. Según se indica por la referencia 522, el dispositivo 200 puede calcular una mezcla 234 del certificado seleccionado y puede almacenar la mezcla 234 en la memoria 206.

El dispositivo 200 puede llevar a cabo tan solo una de las cajas 520 y 522, o puede llevar a cabo las dos.

Se contemplan muchas modificaciones en este método. Por ejemplo, el requisito de que un certificado instalado en la SC 400 se utilice para un propósito particular puede ser permitido por el usuario del dispositivo 200, en lugar de desde una política de seguridad 220. En otro ejemplo, si el dispositivo 200 ya ha importado los certificados desde la SC 400 (para otros propósitos), entonces el dispositivo 200 puede determinar ya, tras lo indicado por la referencia 500, que no se ha instalado ningún certificado para este propósito particular en la SC 400.

La Figura 6 muestra un diagrama de flujo de otro método proporcionado a modo de ejemplo para permitir el uso de un certificado almacenado en una tarjeta inteligente para llevar a cabo una operación que requiere un certificado particular. El dispositivo 200 puede haber sido actualizado o renovado y la información acerca del certificado particular, o incluso una copia del certificado particular almacenada en el dispositivo 200, puede haber sido borrada del dispositivo 200 durante la actualización. Según se indica por la referencia 600, un usuario acopla la SC 400 al SCR 300 y el SCR 300 al dispositivo 200. Según se indica por la referencia 602, el dispositivo 200 verifica si reconoce la tarjeta inteligente 400. Por ejemplo, el dispositivo 200 puede leer el identificador 410 de tarjeta inteligente en la SC 400 y puede compararlo con un identificador 232 de tarjeta inteligente previamente almacenado en la memoria 206.

Según se indica por la referencia 604, el dispositivo 200 insta al usuario a introducir una palabra de paso para autentificación y, conforme a lo indicado por la referencia 606, el dispositivo 200 hace pasar la palabra de paso introducida por el usuario a la SC 400 para su verificación. Conforme a lo indicado por la referencia 608, la SC 400 verifica si la palabra de paso introducida es idéntica a la palabra de paso 414 para autentificación.

Si, como se muestra por la referencia 610, una copia del certificado particular está almacenada en el área 232, el método puede continuar por lo indicado por la referencia 612. Si no se ha almacenado una copia del certificado en el área 232 y no se ha almacenado una mezcla del certificado particular en la mezcla 234, el método puede finalizar, tal y como se muestra por la referencia 614. Sin embargo, si hay una mezcla del certificado particular almacenada en la mezcla 234, el método puede continuar por lo indicado por la referencia 616.

Según se indica por la referencia 616, el dispositivo importa uno de los certificados almacenados en la SC 400, y, conforme a lo indicado por la referencia 618, el dispositivo 200 calcula una mezcla del certificado importado. Según lo indicado por la referencia 620, el dispositivo 200 compara la mezcla calculada con la mezcla 234. Si la mezcla calculada no es idéntica a la mezcla 234, el método puede continuar proseguir por lo indicado por la referencia 616, para comprobar otros certificados almacenados en la SC 400, o bien puede terminar, si todos los certificados de la SC fueron comprobados y no se encontró ninguna coincidencia. Aunque el diagrama de flujo de la Figura 6 muestra el dispositivo importando los certificados uno de cada vez, el dispositivo puede importar todos los certificados y, seguidamente, comprobarlos de una sola vez.

Si, sin embargo, el dispositivo 200 importa un certificado y encuentra que la mezcla del certificado es idéntica a la mezcla 234, según se indica por la referencia 622, el dispositivo 200 puede almacenar el certificado importado en el área 232. El método puede continuar por lo indicado por la referencia 612.

Según se indica por la referencia 612, el dispositivo 200 genera una pregunta aleatoria y envía la pregunta y una identificación del certificado almacenado en el área 232 a la SC 400. Utilizando la clave privada emparejada con el certificado seleccionado, la SC 400 firma la pregunta según lo indicado por la referencia 624, y, de acuerdo con lo indicado por la referencia 626, la SC 400 la pregunta firmada al dispositivo 200.

Utilizando el certificado almacenado en el área 232, el dispositivo 200 verifica, según lo indicado por la referencia 628, que la pregunta se ha firmado con la clave privada emparejada con ese certificado. Si la pregunta se ha firmado con la clave privada emparejada con el certificado almacenado en el área 232, el dispositivo 200 permite una operación deseada, por ejemplo, desbloquear el dispositivo 200 para su uso por parte del usuario.

Instrucciones ejecutables por computadora para llevar a cabo cualesquiera partes del método anteriormente descrito, pueden ser almacenadas en una forma de medio legible por computadora. Los medios legibles por computadora incluyen medios volátiles y no volátiles, extraíbles y no extraíbles, implementados en cualquier método o tecnología para el almacenamiento de información, tal como instrucciones legibles por computadora, estructuras de datos, módulos de programa u otros datos. Los medios legibles por computadora incluyen, si bien no se limitan a ellos, memoria de acceso aleatorio (RAM –"random access memory"), memoria de solo lectura (ROM), ROM programable y borrable eléctricamente (EEPROM), memoria de refrescamiento por impulsos u otra tecnología de memoria, ROM de disco compacto (CD ROM), discos versátiles digitales (DVD –"digital versatile disks") u otro dispositivo de almacenamiento óptico, casetes magnéticas, cinta magnética, dispositivo de almacenamiento de disco magnético u otros dispositivos de almacenamiento magnéticos, o cualquier otro medio que pueda utilizarse para almacenar las instrucciones deseadas y al que pueda accederse por el dispositivo 108 y/o el SCR 104, incluyendo por la Internet u otras formas de acceso por red informática.

Si bien la materia objeto se ha descrito en un lenguaje específico para características estructurales y/o acciones metodológicas, ha de comprenderse que la materia objeto que se define en las reivindicaciones que se acompañan no está necesariamente limitada a las características o acciones específicas anteriormente descritas. En lugar de ello, las características y acciones específicas que se han descrito en lo anterior se divulgan como formas ejemplares de implementar las reivindicaciones.

REIVINDICACIONES

1.- Un método, en un dispositivo computerizado (108, 200) acoplado o conectado a un lector (104, 300) de tarjeta inteligente, de tal manera que el método comprende:

almacenar en una memoria (206) del dispositivo (200) una política de seguridad que requiere un certificado (420) de clave pública para la autentificación de un usuario, una pregunta / respuesta de autentificación de dos factores, encriptación o cifrado de información, información de firma, seguridad de exploración de web, registro de entrada en un servicio de web y/o facilitación del acceso a una red o a un dispositivo;
identificar que una tarjeta inteligente (102, 400) acoplada a dicho lector (104, 300) de tarjeta inteligente no almacena un certificado de clave pública que se requiere por parte de la política de seguridad almacenada;
instar a un usuario de dicho dispositivo (108, 200) a seleccionar un certificado de clave pública de entre uno o más certificados (420) de clave pública almacenados en la tarjeta inteligente (102, 400) acoplada a dicho lector (104, 300) de tarjeta inteligente; e
importar dicho certificado de clave pública seleccionado a dicho dispositivo (108, 200).

2.- El método de acuerdo con la reivindicación 1, que comprende adicionalmente:

almacenar dicho certificado y dicho dispositivo (108, 200).

3.- El método de acuerdo con la reivindicación 2, que comprende adicionalmente:

enviar una pregunta a dicha tarjeta inteligente (102, 400);
identificar dicho certificado para dicha tarjeta inteligente (102, 400);
recibir una versión firmada de dicha pregunta desde dicha tarjeta inteligente (102, 400); y
utilizar dicho certificado almacenado en dicho dispositivo (108, 200) para verificar que dicha versión firmada se ha firmado utilizado una clave privada (418) emparejada con dicho certificado (420).

4.- El método de acuerdo con la reivindicación 3, que comprende adicionalmente:

permitir una operación particular en dicho dispositivo (108, 200) si se ha verificado dicha versión firmada.

5.- El método de acuerdo con la reivindicación 4, en el cual dicha operación particular es desbloquear dicho dispositivo (108, 200) o acceder a información o a una red a través de dicho dispositivo (108, 200).

6.- El método de acuerdo con una cualquiera de las reivindicaciones 1 a 5, que comprende adicionalmente:

requerir a dicho usuario que proporcione una palabra de paso para autentificación;
comparar dicha palabra de paso con una palabra de paso para autentificación (414) almacenada en dicha tarjeta inteligente (102, 400); e
importar dicho certificado únicamente si dicha palabra de paso proporcionada y dicha palabra de paso para autentificación (414) almacenada en dicha tarjeta inteligente (102, 400) sin idénticas.

7.- El método de acuerdo con una cualquiera de las reivindicaciones 1 a 6, que comprende adicionalmente:

calcular una mezcla (234) de dicho certificado; y
almacenar dicha mezcla (234) en dicho dispositivo (108, 200).

8.- El método de acuerdo con la reivindicación 7, que comprende adicionalmente:

importar otro certificado;
calcular una mezcla de dicho otro certificado; y
comparar dicha mezcla de dicho otro certificado con dicha mezcla almacenada (234).

9.- El método de acuerdo con la reivindicación 8, que comprende adicionalmente:

si dicha mezcla de dicho otro certificado y dicha mezcla almacenada (234) son idénticas, utilizar dicho otro certificado para un propósito particular en dicho dispositivo (108, 200).

10.- Un medio legible por computadora que tiene en él instrucciones ejecutables por computadora, las cuales, cuando son ejecutadas por un dispositivo computerizado (108, 200) que está acoplado o conectado a un lector de tarjeta inteligente (104, 300), dan como resultado el método de acuerdo con una cualquiera de las reivindicaciones 1 a 9.

11.- Un dispositivo computerizado (200) que comprende:

una interfaz de comunicación (202) a través de la cual dicho dispositivo (20) es capaz de acoplarse o conectarse a un lector (104, 300) de tarjeta inteligente;
una interfaz (224) de introducción por parte del usuario;
un procesador (204) conectado a dicha interfaz de comunicación (202) y a dicha interfaz (224) de introducción por parte del usuario; y
una memoria (206) conectada a dicho procesador (204), de tal manera que dicha memoria (206) es capaz de almacenar medios de código ejecutables (230), los cuales, cuando se ejecutan por dicho procesador (204), están dispuestos para llevar a cabo las etapas de método de una cualquiera de las reivindicaciones 1 a 9.

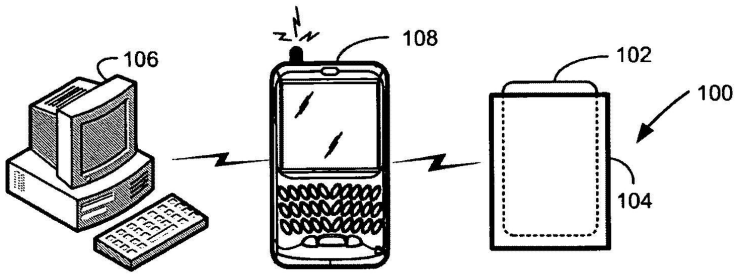

FIG. 1

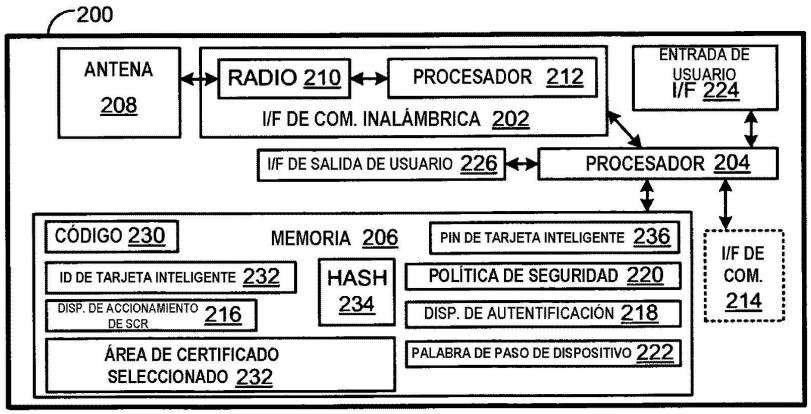

FIG. 2

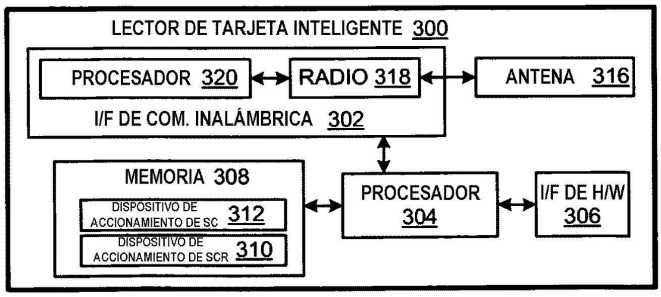

FIG. 3

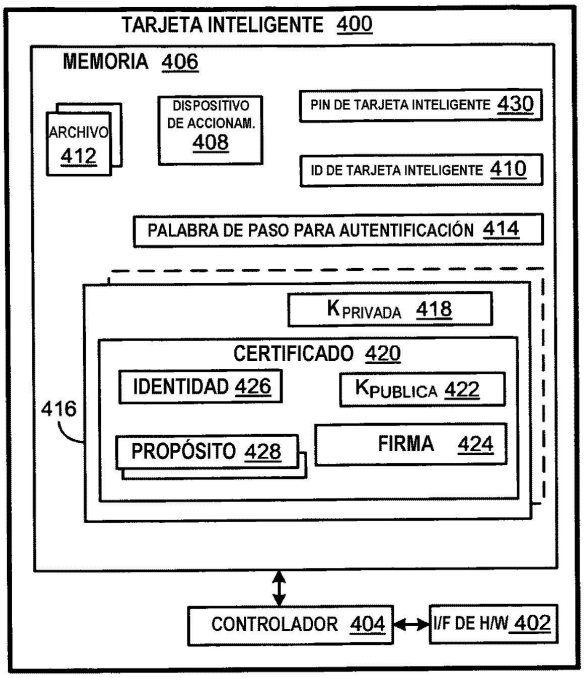
TARJETA INTELIGENTE 400
MEMORIA 406
ARCHIVO 412
DISPOSITIVO DE ACCIONAM. 408
PIN DE TARJETA INTELIGENTE 430
ID DE TARJETA INTELIGENTE 410
PALABRA DE PASO PARA AUTENTIFICACIÓN 414
K PRIVADA 418
CERTIFICADO 420
IDENTIDAD 426
K PUBLICA 422
416
PROPÓSITO 428
FIRMA 424
CONTROLADOR 404
I/F DE H/W 402

FIG. 4

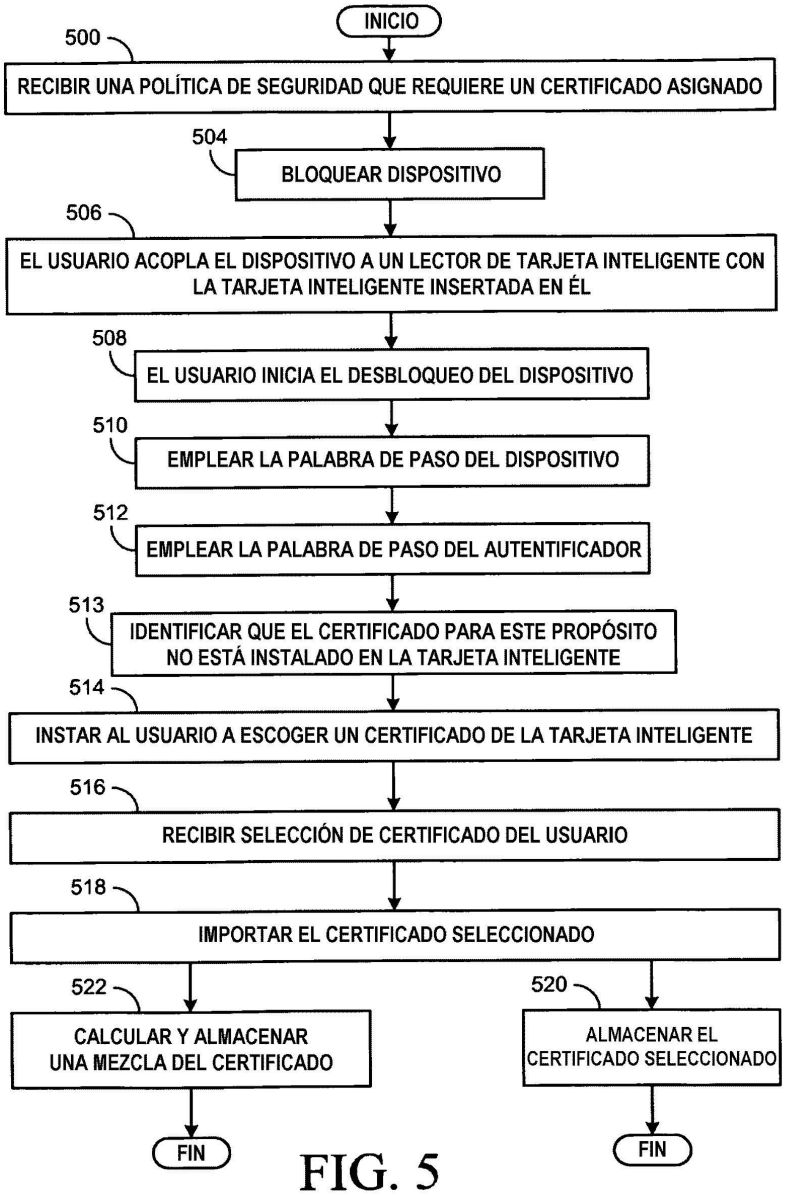
INICIO
500
RECIBIR UNA POLÍTICA DE SEGURIDAD QUE REQUIERE UN CERTIFICADO ASIGNADO
504
BLOQUEAR DISPOSITIVO
506
EL USUARIO ACOPLA EL DISPOSITIVO A UN LECTOR DE TARJETA INTELIGENTE CON LA TARJETA INTELIGENTE INSERTADA EN ÉL
508
EL USUARIO INICIA EL DESBLOQUEO DEL DISPOSITIVO
510
EMPLEAR LA PALABRA DE PASO DEL DISPOSITIVO
512
EMPLEAR LA PALABRA DE PASO DEL AUTENTIFICADOR
513
IDENTIFICAR QUE EL CERTIFICADO PARA ESTE PROPÓSITO NO ESTÁ INSTALADO EN LA TARJETA INTELIGENTE
514
INSTAR AL USUARIO A ESCOGER UN CERTIFICADO DE LA TARJETA INTELIGENTE
516
RECIBIR SELECCIÓN DE CERTIFICADO DEL USUARIO
518
IMPORTAR EL CERTIFICADO SELECCIONADO
522
CALCULAR Y ALMACENAR UNA MEZCLA DEL CERTIFICADO
520
ALMACENAR EL CERTIFICADO SELECCIONADO
FIN
FIN

FIG. 5

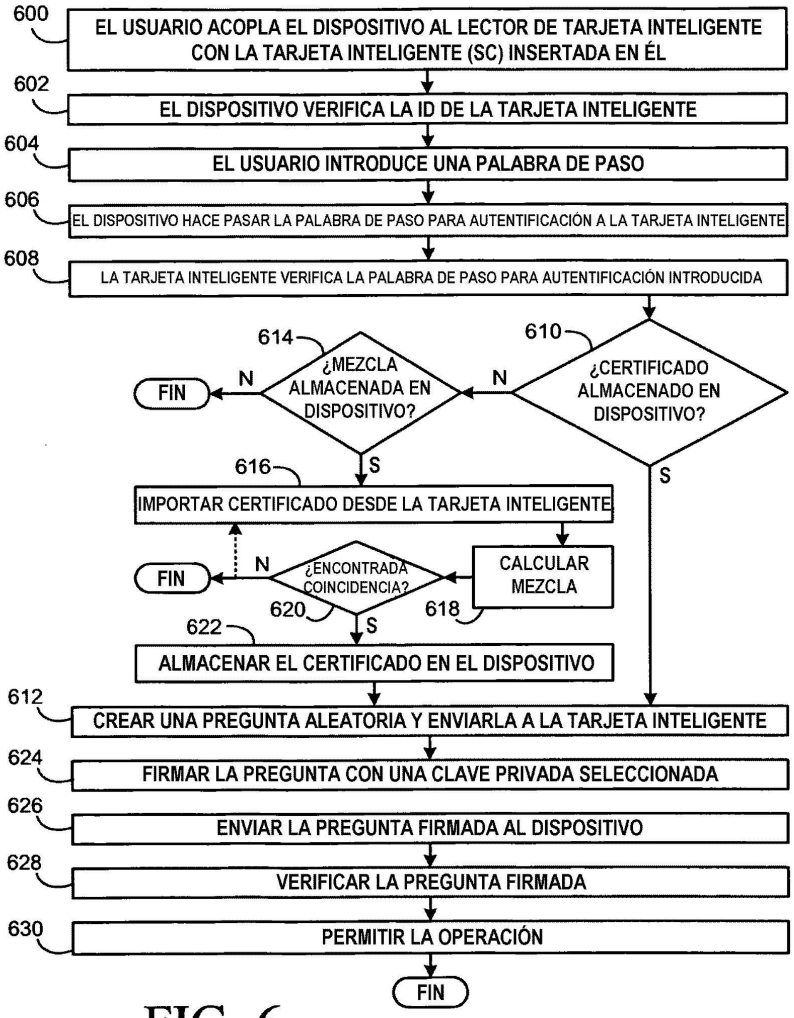
600
EL USUARIO ACOPLA EL DISPOSITIVO AL LECTOR DE TARJETA INTELIGENTE CON LA TARJETA INTELIGENTE (SC) INSERTADA EN ÉL
602
EL DISPOSITIVO VERIFICA LA ID DE LA TARJETA INTELIGENTE
604
EL USUARIO INTRODUCE UNA PALABRA DE PASO
606
EL DISPOSITIVO HACE PASAR LA PALABRA DE PASO PARA AUTENTIFICACIÓN A LA TARJETA INTELIGENTE
608
LA TARJETA INTELIGENTE VERIFICA LA PALABRA DE PASO PARA AUTENTIFICACIÓN INTRODUCIDA
610
¿CERTIFICADO ALMACENADO EN DISPOSITIVO?
N
S
614
¿MEZCLA ALMACENADA EN DISPOSITIVO?
N
S
FIN
616
IMPORTAR CERTIFICADO DESDE LA TARJETA INTELIGENTE
CALCULAR MEZCLA
618
¿ENCONTRADA COINCIDENCIA?
N
S
620
FIN
622
ALMACENAR EL CERTIFICADO EN EL DISPOSITIVO
612
CREAR UNA PREGUNTA ALEATORIA Y ENVIARLA A LA TARJETA INTELIGENTE
624
FIRMAR LA PREGUNTA CON UNA CLAVE PRIVADA SELECCIONADA
626
ENVIAR LA PREGUNTA FIRMADA AL DISPOSITIVO
628
VERIFICAR LA PREGUNTA FIRMADA
630
PERMITIR LA OPERACIÓN
FIN

FIG. 6