(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 662 438**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
H04W 4/00 (2009.01)
H04W 12/02 (2009.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.12.2013 E 13197715 (9)**

(97) Fecha y número de publicación de la concesión europea: **13.12.2017 EP 2747334**

(54) Título: **Sistema de almacenamiento seguro que comprende un dispositivo de seguridad virtual y un dispositivo de almacenamiento seguro móvil**

(30) Prioridad:

19.12.2012 US 201261739064 P
19.12.2012 EP 12198190

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.04.2018

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
22-24, route de Genève
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es:

PELLETIER, HERVÉ

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Sistema de almacenamiento seguro que comprende un dispositivo de seguridad virtual y un dispositivo de almacenamiento seguro móvil

Dominio técnico

[0001] La presente invención se refiere al dominio del acceso controlado a información digital, más particularmente al almacenamiento seguro o copia de seguridad de dicha información.

Estado de la técnica

[0002] No se puede confiar solamente en la memoria humana, que es falible por naturaleza, para recordarlo todo. Esta ha sido una observación fundamental que llevó a la gente a encontrar vías más fiables para recordar la información. Hoy en día la gente tiene que recordar cada vez más cosas como nombres de usuario, contraseñas, números de identificación personal (PIN), números de cuenta y demás. Esto se puede describir como información privada e incluye información que es preferiblemente exclusiva pencara esa persona y sirve para identificarla positivamente. Además, normalmente resulta ventajoso que este tipo de información se mantenga en secreto, ya que su divulgación podría permitir a una tercera parte tener acceso a la cuenta bancaria de esa persona o, por otro lado, hacerse pasar esa tercera parte por esa persona o tener acceso a otra información personal que la persona prefiere ocultar.

[0003] Conociendo la pobre fiabilidad de la memoria de alguna gente, la gente ha recurrido a escribir tal información privada en pedazos de papel. Para mayor seguridad, el papel a veces se guarda en una caja fuerte o en otro lugar seguro de otra manera. Más recientemente, en vez de usar papel, la información privada frecuentemente se almacena en un ordenador en formato de texto claro. Por ordenador se entiende que incluye los dispositivos móviles tales como asistentes digitales personales (PDA) y teléfonos móviles, por ejemplo. Para mayor seguridad, la información almacenada frecuentemente se encripta utilizando los sistemas de encriptación disponibles clásicamente, pero nuevamente se requiere generalmente una contraseña o frase de acceso para desencriptar la información, lo que conduce a un escenario clásico del huevo y la gallina en cuanto a dónde guardar la contraseña/frase de acceso.

[0004] A pesar de los inconvenientes asociados a guardar la información privada en un dispositivo móvil tal como un teléfono móvil, sigue habiendo una gran ventaja que se extrae de tal técnica desde el punto de vista de la conveniencia, ya que mucha gente tiene su teléfono móvil con ellos la mayoría de las veces. Sí que existe el inconveniente de que una pérdida accidental del dispositivo móvil produce la pérdida de toda la información privada. Este inconveniente se puede superar prestando atención minuciosa a hacer copias de seguridad del dispositivo móvil en un medio de copia de seguridad seguro. Existe, por lo tanto, un fuerte incentivo para recurrir a esta técnica de almacenar información privada en dispositivos móviles.

[0005] Como se reconoce por el solicitante del número de publicación de solicitud de patente estadounidense 2009/0075630 A1, el uso de la técnica anteriormente mencionada no hace nada para proteger la información privada de las miradas curiosas de los intentos de terceras partes sin escrúpulos para acceder a la información privada así almacenada, especialmente cuando la tercera parte encuentra un dispositivo móvil de una persona que lo ha perdido. Se dice que la solución generalmente reconocida para esto, que sería mantener la información privada solo en el formato encriptado hasta las veces en las que el usuario requiriera acceder a la misma, gasta mucho tiempo, es poco práctica y demasiado intensiva para el procesador/memoria para hacerlo en un dispositivo móvil. A modo de una solución para esto, el documento divulga mecanismos que permiten a los usuarios proteger los datos almacenados en teléfonos móviles activando remotamente una aplicación que encripta datos y luego elimina la clave de encriptación de la memoria del teléfono móvil. Los datos encriptados se pueden enviar a un servidor como mecanismo de copia de seguridad. Una clave de encriptación o bien se recibe desde el servidor o bien se genera por el teléfono móvil y se comunica al servidor. El servidor se configura para autentificar usuarios. El servidor se puede además configurar para devolver los datos al teléfono móvil transmitiendo los ficheros vía una red inalámbrica, como la red de telefonía móvil. Los mecanismos se pueden configurar para la ejecución regular periódica de la encriptación y copia de seguridad así descritas para que se realicen automáticamente en los ficheros de datos seleccionados. La desventaja de este sistema es que para ser capaz de desencriptar los ficheros encriptados, el usuario necesita reinsertar la clave de encriptación.
Para hacer eso, debe solicitarla al servidor y se tiene que autentificar él mismo al servidor. Esto conduce otra vez al problema del huevo y la gallina en el que el usuario tiene que recordar una contraseña para la autentificación.

[0006] El número de publicación de solicitud de patente estadounidense 2009/0075630 A1 describe una técnica de copia de seguridad segura para usar con teléfonos móviles, donde una aplicación de encriptación en el teléfono se activa remotamente para permitir la encriptación de la información privada por el teléfono. La información privada del teléfono móvil también se puede enviar a un servidor remoto como copia de seguridad, bien en la forma clara o en la forma encriptada. Una vez que la encriptación se ha completado, la información privada clara y la clave de encriptación se eliminan de la memoria del teléfono.

[0007] El sistema anterior presenta las desventajas de que los datos encriptados permanecen en el teléfono y la encriptación se realiza por el teléfono. Además, la información privada se puede interceptar por una tercera parte maliciosa mientras se comunica entre el teléfono y el servidor. De forma similar, la clave de encriptación se puede interceptar mientras se envía al teléfono. Finalmente, la desencriptación de la información privada también se hace en el teléfono. Una desventaja adicional es que se le tiene que pedir al usuario que ejecute una copia de seguridad, que, como se describe en la publicación, requiere pasos especiales que se deben tomar para esconder de un sujeto malicioso cualquier indicación de que los datos están en proceso de ser copiados.

Breve resumen de la invención

[0008] Para superar algunas de las desventajas existentes en la técnica anterior para la protección fiable de la información privada, la presente invención proporciona un dispositivo de almacenamiento móvil y un dispositivo de seguridad virtual que pueden trabajar juntos al menos temporalmente para proporcionar un almacenamiento seguro y la recuperación de un valor privado. En el sistema según una forma de realización de la presente invención, el dispositivo de comunicaciones móvil se utiliza para proporcionar el valor privado al dispositivo de seguridad virtual y para memorizar una versión encriptada del valor privado. La encriptación se hace por el dispositivo de seguridad virtual, utilizando una clave secreta que corresponde con el dispositivo de comunicaciones móvil, donde el valor privado encriptado se envía de nuevo al dispositivo de comunicaciones móvil. El valor privado se puede restaurar cuando el dispositivo móvil envía el valor privado encriptado de nuevo al dispositivo de seguridad virtual. El dispositivo de seguridad virtual autoriza entonces el acceso del dispositivo móvil al valor privado desencriptado. Esta autorización se puede conseguir mediante el simple envío por parte del dispositivo de seguridad virtual del valor privado desencriptado de nuevo al dispositivo móvil o el envío del valor encriptado y la clave secreta de nuevo al dispositivo móvil, donde el dispositivo móvil completa la desencriptación. Las comunicaciones mencionadas anteriormente solo pueden ocurrir cuando los dos dispositivos están dentro de una distancia predeterminada el uno del otro, donde esta distancia es lo suficientemente baja como para requerir que el dispositivo de virtual, el dispositivo móvil y, por deducción, el usuario, estén todos simultáneamente en el hogar del usuario, por ejemplo. Preferiblemente el canal de comunicación entre los dos dispositivos es un canal seguro.

[0009] Según un primer aspecto de la presente invención, se proporciona un método para almacenar de forma segura un valor privado, donde el método utiliza un sistema que comprende:

un dispositivo de almacenamiento móvil con un parámetro de identificación, donde el dispositivo de almacenamiento móvil comprende una primera interfaz de comunicaciones inalámbricas configurada para establecer una conexión inalámbrica de proximidad local con un dispositivo compatible; y
un dispositivo de seguridad virtual configurado para llevar a cabo funciones criptográficas, donde el dispositivo de seguridad virtual comprende:

una segunda interfaz de comunicaciones inalámbricas configurada para establecer una conexión inalámbrica de proximidad local con un dispositivo compatible;
un módulo de seguridad; y
una memoria segura para almacenar al menos una clave secreta que corresponde con el parámetro de identificación de al menos un dispositivo de almacenamiento móvil;

donde el método comprende:

el establecimiento de un canal de comunicación inalámbrica de proximidad local entre la primera interfaz de comunicaciones inalámbricas y la segunda interfaz de comunicaciones inalámbricas;
el envío del parámetro de identificación del dispositivo de almacenamiento móvil al dispositivo de seguridad virtual vía el canal de comunicación inalámbrica de proximidad local;
el envío del valor privado del dispositivo de almacenamiento móvil al dispositivo de seguridad virtual vía el canal de comunicación inalámbrica de proximidad local;
la encriptación, por el módulo de seguridad, del valor privado utilizando la clave secreta que corresponde con el parámetro de identificación del dispositivo de almacenamiento móvil para dar la versión encriptada del valor privado; y
el envío de la versión encriptada del valor privado del dispositivo de seguridad virtual al dispositivo de almacenamiento móvil.

[0010] Según otro aspecto de la presente invención, se ha proporcionado un sistema de almacenamiento seguro que comprende un dispositivo de seguridad virtual y un dispositivo de almacenamiento móvil; donde el dispositivo de almacenamiento móvil tiene un parámetro de identificación y comprende una primera interfaz de comunicaciones inalámbricas configurada para funcionar según un estándar de comunicación inalámbrica de proximidad;
donde el dispositivo de seguridad virtual comprende:

una segunda interfaz de comunicaciones inalámbricas configurada para funcionar según el estándar de comunicación inalámbrica de proximidad y para establecer así un canal de comunicación inalámbrica de proximidad local entre el dispositivo de seguridad virtual y el dispositivo de almacenamiento móvil;
una memoria segura para almacenar al menos una clave secreta que corresponde con el parámetro de identificación del dispositivo de almacenamiento móvil; y
un módulo de seguridad configurado para:

recibir el valor privado del dispositivo de almacenamiento móvil vía el canal de comunicación inalámbrica de proximidad local; y
encriptar el valor privado utilizando la clave secreta que corresponde con el parámetro de identificación del dispositivo de almacenamiento móvil.

[0011] Las formas de realización de la presente invención proporcionan ventajas, entre otras, la de que la clave de desencriptación no necesita almacenarse en el dispositivo de almacenamiento móvil y, de hecho, se puede eliminar activamente del dispositivo de almacenamiento móvil cuando el usuario retira el dispositivo del entorno seguro proporcionado por el hogar del usuario, reduciendo así inmensamente la posibilidad de que un tercero malicioso descubra la clave de desencriptación desde dentro de un entorno relativamente inseguro del dispositivo de almacenamiento móvil en cualquier momento fuera del hogar. En estas formas de realización, la desencriptación de los valores privados solo se puede realizar mientras el usuario está en su hogar, o al menos lo suficiente cerca al dispositivo de seguridad virtual como para que funcione la interfaz inalámbrica de proximidad cercana.

[0012] Según otras formas de realización, ventajosamente, la clave de desencriptación no necesita nunca llegar a salir del entorno seguro representado por el dispositivo de seguridad virtual. Ya que la clave de desencriptación nunca se pasa al dispositivo de almacenamiento móvil, esto elimina la posibilidad de que un tercero malicioso descubra la clave de desencriptación mientras se pasa del dispositivo de seguridad virtual al dispositivo de almacenamiento móvil y también elimina la posibilidad de que la clave de desencriptación sea descubierta a partir del dispositivo de almacenamiento móvil en cualquier momento. Los dispositivos de comunicaciones móviles estándar, tales como teléfonos móviles o dispositivos de tabletas, etc., sin modificación particular se pueden usar, ya que la responsabilidad de realizar las funciones criptográficas recae en el dispositivo de seguridad virtual. Un descodificador u otro dispositivo de recepción de audio/video o servidor multimedia, adaptado según las formas de realización de la invención, se puede usar convenientemente como un dispositivo de seguridad virtual.

[0013] Estos y otros aspectos de la presente invención se describirán a continuación.

Breve descripción de los dibujos

[0014] La presente invención se entenderá mejor gracias a la descripción detallada que sigue y al dibujo anexo, que se da como ejemplos no limitativos de formas de realización de la invención, donde:

la figura 1 muestra un diagrama de un sistema donde se puede emplear una forma de realización de la presente invención.
la figura 2 muestra un diagrama de una secuencia de eventos que ocurren en un sistema donde se puede emplear una forma de realización de la presente invención.

Descripción detallada

[0015] La presente invención se beneficia del hecho, entre otros, de que la autentificación suficientemente fiable se puede conseguir de maneras relativamente simples dependiendo del entorno y las circunstancias bajo las cuales debe ocurrir la autentificación.

[0016] Es un deseo común para la gente guardar determinados detalles privados o valores privados de manera que sean convenientemente accesibles, aunque seguros. Tales valores privados pueden tomar la forma de una contraseña, una frase de acceso, un ID y/o una contraseña de cuenta, números de tarjetas de crédito, etc. Estos valores, si los descubre una tercera parte maliciosa, presentan una oportunidad para que esa tercera parte haga algún daño. Las recompensas percibidas por esa tercera parte, sin embargo, son normalmente limitadas en el caso de valores privados pertenecientes a un particular, así que, por la misma cantidad de trabajo para intentar descubrir tal información, la tercera parte puede decidir tratar de intentar descubrir otras informaciones donde los beneficios puedan multiplicarse. Por ejemplo, si el descubrimiento de una clave secreta pudiera llevar a la tercera parte a poder vender copias piratas de un programa de software o de una película, entonces eso podría suponer un alto incentivo para la tercera parte. Los valores privados aquí discutidos, sin embargo, suponen un incentivo pequeño para una tercera parte maliciosa, pero aun así requieren ser lo suficientemente seguros para disuadir a la tercera parte de intentar acceder a los valores privados.

[0017] Con esto en mente, se proponen formas de realización de la presente invención donde la seguridad se proporciona basándose en que, en general, un usuario de un sistema donde se emplea una forma de realización de la presente invención tendrá asegurado generalmente que solo un número limitado de gente tendrá acceso a su hogar. Además, en circunstancias normales, solo el usuario tendrá acceso al dispositivo de comunicaciones móvil personal del usuario. Aquí, un dispositivo de comunicaciones se puede entender que es un asistente digital personal, un teléfono móvil o cualquier dispositivo móvil capaz de realizar una comunicación inalámbrica con un servidor. Por servidor, este puede significar cualquier dispositivo de computación con conexión inalámbrica tal como un ordenador personal o, como en formas de realización particulares de la presente invención, un descodificador o cualquier dispositivo de recepción de multimedia en reproducción, especialmente aquellos que están equipados con una tarjeta inteligente o un módulo de seguridad o que son capaces de otro modo de realizar funciones criptográficas. Basándose en estas dos condiciones simultáneas, es decir, tener acceso a unas instalaciones particulares tales como un hogar particular y tener acceso a un dispositivo de comunicación móvil particular tal como un teléfono inteligente particular, se establece un grado de seguridad suficiente en cuanto a que un dispositivo de recepción particular en el hogar particular será capaz de autentificar un dispositivo móvil particular con un grado razonable de confianza. Según una forma de realización de la presente invención, los medios de comunicación inalámbrica entre el dispositivo de recepción y el dispositivo de comunicaciones móvil se limitan adicionalmente para que sean de un tipo de proximidad, puesto que tienen un alcance limitado. Un ejemplo de un tipo de proximidad de canal de comunicaciones inalámbricas es uno que es compatible con Bluetooth. Se puede utilizar cualquier tipo de medios de comunicación de proximidad. Ventajosamente, uno que cumple con el estándar de Comunicación de Campo Cercano (NFC), cuando se usa en formas de realización de la presente invención, limita las posibilidades de establecer una comunicación con el dispositivo de recepción por un dispositivo de comunicación móvil para que sean solo aquellos que están a unos pocos centímetros del dispositivo de recepción. Esto proporciona una garantía de que el dispositivo de comunicación móvil y su usuario realmente están en cercana proximidad entre sí para que se establezca una conexión. Tales canales de comunicaciones son, por lo tanto, también conocidos como canales de comunicaciones de proximidad local. Por consiguiente, las interfaces de comunicación inalámbrica conformes con el estándar wifi proporcionan una desventaja en un sistema según las formas de realización de la presente invención en tanto que la condición de que el usuario esté muy próximo, un requisito que se satisface cuando el usuario está en su propio hogar, se impone, por lo tanto, menos estrictamente.

[0018] Se puede observar entonces que, dadas las limitaciones anteriores, las terceras partes maliciosas que buscan aprovecharse de los valores privados seguros según una forma de realización de la presente invención, para conseguir sus objetivos, deberían demostrar las improbables características simultáneas de tener acceso al hogar del usuario y tener en posesión el teléfono móvil del usuario.

[0019] Según una forma de realización de la presente invención, se proporciona un sistema que comprende un descodificador y al menos un teléfono móvil. El descodificador se configura según sistemas de TV de pago conocidos y comprende así un módulo de seguridad o una tarjeta inteligente y se configura para ejecutar operaciones seguras tales como realizar funciones criptográficas y para almacenar de forma segura claves criptográficas y otros valores secretos en una memoria segura. Preferiblemente, el descodificador permanece encendido en todo momento, pero es al menos capaz de funcionar cuando el usuario llega al hogar o poco después. El descodificador debería permanecer encendido siempre y cuando el usuario desee usarlo de la manera aquí descrita. El sistema puede comprender más de un teléfono móvil, que normalmente pertenecen a usuarios diferentes siempre y cuando cada teléfono móvil se pueda identificar de forma unívoca. Un teléfono móvil configurado para funcionar según las formas de realización de la presente invención requiere ser primero registrado por el sistema. Siempre y cuando un teléfono móvil registrado y su usuario respectivo estén dentro de una distancia predeterminada del descodificador, entonces ese usuario será capaz de acceder de forma segura a cualquiera de sus valores privados que se han almacenado en el sistema. Por teléfono móvil, en el contexto de la presente invención, se entiende que incluye cualquier dispositivo de comunicación móvil personal como teléfonos móviles, PDA, ordenadores portátiles, tabletas, etc. Tales dispositivos son normalmente solo usados por una persona y son, por tanto, personales o privados. Por descodificador se entiende que incluye cualquier dispositivo de recepción de contenido multimedia capaz de establecer un canal de comunicación inalámbrica como se ha descrito en este documento.

[0020] El proceso para registrar un teléfono móvil según las formas de realización de la presente invención se describe ahora en parte. Tal y como se ha mencionado, el descodificador del sistema anteriormente descrito comprende una tarjeta inteligente, preferiblemente emparejada o asociada de otro modo al descodificador. La tarjeta inteligente se configura para realizar funciones criptográficas asimétricas o simétricas y como tal se asocia con una clave pública, donde la clave pública tiene elementos de clave pública (e,N). Parte del procedimiento para registrar un teléfono móvil requiere que la clave pública asociada a la tarjeta inteligente se guarde en el teléfono móvil. Esto solo necesita hacerse una vez y se puede realizar, por ejemplo, vía internet cuando el teléfono móvil comprende además una interfaz de comunicación de internet. Según una forma de realización, el usuario establece una conexión entre el teléfono móvil y el descodificador (bien de forma inalámbrica o vía internet cuando el descodificador comprende además una conexión a internet) para recibir la clave pública desde el descodificador. Según otra forma de realización, el sistema comprende además un servidor de clave pública y el usuario establece una conexión entre el teléfono móvil y el servidor de clave pública vía internet. El usuario es

así capaz de almacenar la clave pública en el teléfono móvil, realizando así la primera parte del registro del teléfono móvil. La segunda parte se describirá en un apartado más adelante de la discusión.

[0021] Siempre y cuando el teléfono móvil esté lo suficientemente cerca del descodificador como para estar en el alcance operativo de la interfaz de comunicación del sistema (unos pocos centímetros para una interfaz de comunicación inalámbrica compatible con NFC) se puede establecer un canal inalámbrico seguro entre el teléfono móvil y (la tarjeta inteligente de) el descodificador. Para hacer el canal inalámbrico seguro, se puede utilizar cualquiera de las técnicas conocidas. Por ejemplo, el teléfono móvil genera un valor aleatorio x según el protocolo Diffie-Hellman y computa un secreto s = g^x mod p, donde p y g son parámetros de grupo (primo y generador, respectivamente) del protocolo Diffie-Hellman. Utilizando los elementos de la clave pública almacenada, el teléfono móvil calcula s^e mod N y lo envía, vía el canal de comunicación inalámbrica, a la tarjeta inteligente en el descodificador. Esto evita los llamados ataques "de intermediario". La tarjeta inteligente desencripta el valor recibido desde el teléfono móvil usando su clave privada d y genera un segundo valor aleatorio y. Luego computa una clave de canal Kc mediante Kc = g^(x*y) mod p. La tarjeta inteligente envía g^y mod p de nuevo al teléfono móvil y el teléfono móvil entonces calcula también Kc, ya que ahora puede hacer Kc = g^(x*y) mod p. Kc se vuelve ahora una clave de canal con la cual el canal entre el descodificador y el teléfono móvil puede asegurarse. Esta clave se utiliza para encriptar/desencriptar (utilizando un algoritmo criptográfico simétrico) todos los intercambios adicionales entre el descodificador y el teléfono móvil. Gracias a este canal seguro, se evita la intercepción por terceras partes.

[0022] La figura 1 muestra un diagrama esquemático de un sistema donde se puede emplear una forma de realización de la presente invención. El sistema comprende al menos un dispositivo de comunicaciones móviles (PCD) con un único parámetro de identificación (UID) y un descodificador (STB) con una tarjeta inteligente (SC). En esta forma de realización, el descodificador y la tarjeta inteligente juntos se conocerán como un dispositivo de seguridad virtual (RCV). El dispositivo de comunicaciones móviles (PCD) comprende un primer módulo de interfaz de comunicaciones inalámbricas (WIF1), un procesador capaz de realizar funciones criptográficas y un módulo de memoria (MM1). El dispositivo de seguridad virtual (RCV) comprende un segundo módulo de interfaz inalámbrica (WIF2) y un módulo de generación de claves y comprende además un módulo criptográfico. El sistema se configura de manera que el dispositivo de seguridad virtual (RCV) y el dispositivo de comunicaciones móviles (PCD) sean capaces de establecer un canal de comunicación inalámbrica (SWIF) entre ellos solo si dichos dos dispositivos están dentro de una distancia predeterminada (DMAX) el uno del otro. Preferiblemente tal canal cumple con un estándar NFC o Bluetooth de manera que el canal de comunicación (SWIF) solo se pueda establecer cuando los dos dispositivos estén a unos pocos centímetros entre sí o a varios metros entre sí, respectivamente. Según esta forma de realización, el sistema comprende además un servidor de clave pública (PKS) para proporcionar el dispositivo de comunicaciones móviles (PCD) con la clave pública del dispositivo de seguridad virtual (o la tarjeta inteligente en su interior). El dispositivo de comunicación móvil y el servidor de clave pública se configuran para ser capaces de comunicarse entre sí, preferiblemente vía una conexión a internet, pero esto podría ser cualquiera de los otros medios conocidos. Según otra forma de realización, el dispositivo de seguridad virtual proporciona la clave pública al dispositivo de comunicaciones móvil. Esto se puede realizar vía un segundo canal de comunicación. Se reconoce que resulta ventajoso desde un punto de vista de la seguridad, recurrir sin embargo a los servicios de un servidor de clave pública.

[0023] Como se ha mencionado previamente, siempre que el dispositivo de comunicaciones móviles entre dentro de la distancia predeterminada del dispositivo de seguridad virtual, un canal de comunicación inalámbrico se puede establecer entre los dos dispositivos. Si el registro no se ha completado y el dispositivo de comunicaciones móvil todavía no es conocido para el dispositivo de seguridad virtual, entonces el parámetro de identificación único del dispositivo de comunicaciones móvil no será conocido para el dispositivo de seguridad virtual. Por parámetro de identificación único se hace referencia a un parámetro que se puede usar para identificar positivamente un dispositivo.
Por identificar positivamente se hace referencia a que el dispositivo de seguridad virtual puede conocer con certeza que un dispositivo que presenta el mismo parámetro de identificación único como se ha presentado previamente es, de hecho, el mismo dispositivo que fue presentado previamente. Por esta razón, el término "parámetro de identificación único" se puede sustituir por "parámetro de identificación". Para completar la segunda parte del registro luego, un dispositivo de comunicación móvil tiene que establecer una conexión con el dispositivo de seguridad virtual y comunicar su parámetro de identificación único al dispositivo de seguridad virtual. Para cada parámetro de identificación único de cada dispositivo de comunicaciones móvil en el sistema, el dispositivo de seguridad virtual genera una clave secreta asociada (KSI). Todas las claves secretas asociadas se almacenan en una memoria segura del dispositivo de seguridad virtual. Esto completa la segunda parte del registro.

[0024] Un método para almacenar un valor privado según varias formas de realización de la presente invención incluye enviar el valor privado del dispositivo móvil al dispositivo de seguridad virtual, preferiblemente vía un canal inalámbrico seguro; y encriptar el valor privado en el dispositivo de seguridad virtual utilizando una clave secreta que corresponde con el dispositivo móvil. La clave secreta se almacena de forma segura en el dispositivo de seguridad virtual y no necesita almacenarse en el dispositivo móvil. El valor privado encriptado se envía de nuevo al dispositivo móvil donde se almacena. El valor privado se elimina del dispositivo móvil y se puede

eliminar preferiblemente del dispositivo de seguridad virtual. El valor privado encriptado también se puede eliminar del dispositivo de seguridad virtual, sin embargo, según algunas formas realización se mantiene en el dispositivo de seguridad virtual como una copia de seguridad.

[0025] Siempre que el usuario quiera almacenar un valor privado, se acerca al dispositivo de seguridad virtual con su dispositivo de comunicación móvil hasta que alcanza el alcance predeterminado y establece así un canal seguro entre el dispositivo móvil y el dispositivo de seguridad virtual. El dispositivo móvil envía su parámetro de identificación único al dispositivo de seguridad virtual, que lo autentifica. El valor privado se envía del dispositivo de comunicaciones móvil vía el canal seguro al dispositivo de seguridad virtual donde se encripta bajo la clave secreta que corresponde con el dispositivo de comunicaciones móvil y se envía de nuevo al dispositivo de comunicaciones móvil para almacenarse allí en la forma encriptada. El valor privado se elimina del dispositivo de comunicaciones móvil y el dispositivo de seguridad virtual y, por lo tanto, ya no existe en ninguna parte en formato claro.

[0026] Un valor privado que corresponde con un dispositivo de comunicaciones móvil particular se encripta, por lo tanto, por el dispositivo de seguridad virtual y se almacena en el formato encriptado en el dispositivo móvil. Un método para la restauración del valor privado en el dispositivo móvil según varias formas de realización de la presente invención se describe ahora. La restauración del valor privado puede ocurrir cuando el dispositivo de comunicaciones móvil se encuentra dentro del alcance requerido (DMAX) del dispositivo de seguridad virtual. Siempre que un dispositivo de comunicaciones móviles entre dentro del alcance del dispositivo de seguridad virtual y se establezca un canal de comunicaciones inalámbricas, el dispositivo de seguridad virtual verifica el parámetro de identificación único, recibido del dispositivo de comunicaciones móvil vía el canal de comunicación inalámbrica, verifica si el dispositivo de comunicaciones móvil es conocido o no y verifica su integridad. Para restaurar el valor privado en el dispositivo de comunicaciones móvil, el dispositivo móvil envía la versión encriptada del valor privado de nuevo al dispositivo de seguridad virtual. El dispositivo de seguridad virtual, habiendo completado el control de integridad, sabe qué dispositivo móvil está haciendo la solicitud de restauración y usa la clave secreta que corresponde al dispositivo de comunicaciones móvil para desencriptar el valor privado y envía el valor privado desencriptado de nuevo al dispositivo de comunicaciones móvil vía el canal de comunicaciones inalámbricas. Opcional y ventajosamente, el canal de comunicaciones inalámbricas es seguro como se ha descrito anteriormente, gracias a la clave del canal.

[0027] De esta manera, el dispositivo de comunicaciones móvil ha restaurado un valor privado de una manera segura gracias al canal seguro y además lo ha hecho sin que la clave secreta (KSI) haya salido nunca del entorno seguro del dispositivo de seguridad virtual. Esto se ha hecho de una manera conveniente en tanto que el usuario nunca tiene que recordar ninguna contraseña para autentificarse él mismo al solicitar la restauración del valor privado. Fue suficiente con que el dispositivo de comunicaciones móvil registrado adecuadamente entrara dentro de un corto alcance predeterminado del dispositivo de comunicaciones virtual para que el valor privado fuera transferido automáticamente de una manera segura al dispositivo de comunicaciones móviles. Según otra forma de realización, el dispositivo móvil no necesita solicitar acceder al valor privado enviando la versión encriptada del valor privado de nuevo al dispositivo de seguridad virtual, ya que esto se hace automáticamente siempre que el dispositivo de comunicaciones entra dentro del alcance predeterminado del dispositivo de seguridad virtual. Según esta forma de realización, el dispositivo de seguridad virtual desencripta automáticamente todos los valores privados encriptados en el dispositivo móvil y los envía de vuelta desencriptados. Esta forma de realización puede preferiblemente combinarse con otra forma de realización descrita más adelante donde los valores privados, una vez desencriptados, se asocian con un periodo de vida. De esta manera, siempre que el dispositivo móvil sale de la proximidad del dispositivo de seguridad virtual, entonces todos los valores privados en claro se eliminan del dispositivo móvil.

[0028] Según diferentes formas de realización de la presente invención, son posibles diferentes formas de acceder al valor privado. Según una primera forma de realización, como se ha descrito anteriormente, siempre que el dispositivo móvil y el dispositivo de seguridad estén lo suficientemente cerca entre sí como para que el canal inalámbrico sea establecido, el valor privado se vuelve disponible automáticamente para el dispositivo móvil. Según otra forma de realización, una vez que el canal de comunicación se ha establecido, el dispositivo móvil hace primero una solicitud al dispositivo de seguridad antes de que se le conceda acceso al valor privado. La solicitud incluye el envío por parte del dispositivo móvil de la versión encriptada del valor privado de nuevo al dispositivo de seguridad virtual para que el dispositivo de seguridad virtual lo desencripte utilizando la clave secreta del dispositivo móvil.

[0029] Se entiende que los términos "conceda acceso" y "se vuelve disponible" usados anteriormente ambos cubren la idea de que el dispositivo móvil es autorizado por el dispositivo de seguridad virtual para restaurar una copia clara del valor privado encriptado en su memoria. Según diferentes formas de realización, esto se hace de diferentes formas.
Según una forma de realización, la autorización se da sencillamente por el dispositivo de seguridad virtual que desencripta el valor privado y lo envía vía el canal seguro al dispositivo móvil que lo almacena en su memoria. En otra forma de realización, el dispositivo de seguridad virtual envía la clave secreta y el valor privado encriptado al dispositivo móvil vía el canal seguro y el dispositivo móvil desencripta el valor privado.

[0030] Se adoptan medidas de seguridad adicionales según otra forma de realización de la presente invención, donde la eliminación automática de los valores privados de la memoria del dispositivo móvil se realiza siempre que el dispositivo móvil sale del alcance predeterminado del dispositivo de seguridad virtual. Esto asegura que el valor privado no permanezca en la memoria del dispositivo móvil una vez que el usuario salga de su hogar, por ejemplo.

[0031] Según otra forma de realización de la presente invención, el valor privado, una vez restaurado en el dispositivo móvil, tiene un periodo de vida predeterminado. El periodo de vida predeterminado se puede expresar en términos de una duración predeterminada. Después de que el periodo de vida predeterminado haya transcurrido, el valor privado se elimina de la memoria del dispositivo móvil. Esta forma de realización se puede combinar con la anterior, por lo que incluso si el dispositivo móvil permanece dentro del alcance predeterminado, si el periodo de vida trascurre, entonces el valor privado también se elimina. Las formas de realización de estos dos párrafos (anteriores) tienen variantes donde se combinan con la forma de realización donde la clave secreta se envía al dispositivo móvil. La clave también puede tener un periodo de vida y también se puede eliminar cuando el dispositivo móvil salga de la proximidad predeterminada del dispositivo de seguridad virtual.

[0032] Según una otra forma de realización, combinable con las formas de realización de los dos párrafos anteriores, el periodo de vida predeterminado se puede ampliar. Esto evita que los datos privados se eliminen siempre y cuando el usuario esté en el hogar, por ejemplo. Según esta forma de realización, el periodo de vida predeterminado se prolonga o se extiende de otro modo tantas veces como sea necesario cuando el dispositivo móvil del usuario esté lo suficientemente cerca del dispositivo de seguridad virtual como para que se establezca una conexión. Por ejemplo, si el usuario está autorizado para acceder a su valor privado una primera vez para un periodo de vida predeterminado, se aleja del dispositivo de seguridad virtual por un tiempo que encaja en el periodo de vida (sale del hogar) antes de volver de nuevo dentro del alcance predeterminado del dispositivo de seguridad virtual (vuelve al hogar), entonces el valor privado permanece en el dispositivo móvil. Esto permite la conveniencia de tener acceso a datos menos sensibles aun cuando el usuario sale del hogar. El usuario puede decidir qué información es sensible y cuál no y configurar el sistema para asociar periodos de vida a información diferente de modo que la información sensible se elimine rápidamente mientras que la información menos sensible permanezca durante más tiempo, incluso cuando el usuario salga del hogar.

[0033] La figura 2 muestra procesos que se pueden ejecutar en un sistema donde se emplea una forma de realización de la presente invención. Los procesos se ejecutan en secuencia de arriba a abajo de la figura. El registro del dispositivo móvil se inicia mediante la obtención de la clave pública asociada al dispositivo de seguridad virtual. Esto se puede hacer mediante la intermediación de un servidor de clave pública. El registro se completa cuando el dispositivo móvil se vuelve conocido para el dispositivo de seguridad virtual mediante el envío de su identificador único (parámetro de identificación). Esto también se puede acompañar por una figura de integridad de modo que el dispositivo de seguridad virtual pueda controlar la integridad. El secreto se genera por el dispositivo móvil, que genera un número aleatorio y calcula el secreto s = g^x mod p. s^e mod N (que utiliza la clave pública del servidor de clave) se computa entonces y se envía por el dispositivo móvil. Esto es recibido por el dispositivo de seguridad virtual, que también genera una y aleatoria. El dispositivo de seguridad virtual desencripta (s^e mod N) ^d mod N, donde d es la clave privada del dispositivo de seguridad virtual RSA, y computa g^y mod p, que se envía entonces al dispositivo móvil. Tanto el dispositivo de seguridad virtual como el dispositivo móvil computan la clave del canal como Kc = g^x.y mod p según el protocolo Diffie-Hellman. El dispositivo móvil encripta su parámetro de identidad único y lo envía al dispositivo de seguridad virtual junto con su figura de integridad. El dispositivo de seguridad virtual lo comprueba y ahora sabe con certeza qué clave secreta pertenece al dispositivo móvil. De otro modo genera una clave secreta para ese dispositivo móvil. El dispositivo móvil inicia una solicitud para acceder a la información privada mediante el envío de la información privada encriptada al dispositivo de seguridad virtual. El dispositivo de seguridad virtual puede o bien desencriptar la información privada utilizando la clave secreta del dispositivo móvil o bien enviar la clave de nuevo al dispositivo móvil para que la desencriptación se haga allí. Así, el dispositivo móvil no tiene nunca que almacenar la clave de desencriptación o el valor privado en claro cuando está lejos del dispositivo de seguridad virtual, lo que imparte así la seguridad necesaria y conveniencia.

[0034] Todas las formas de realización anteriormente descritas dependen de la capacidad del dispositivo de seguridad virtual para suministrar su clave pública al dispositivo de almacenamiento móvil en la manera apropiada o, más crucialmente, de la capacidad del dispositivo de seguridad virtual para tener acceso rápido a la clave secreta asociada al dispositivo móvil que pide que un valor privado sea almacenado o retornado. Podría pasar que, debido a algún error catastrófico, el dispositivo de seguridad virtual ya no fuera capaz de proporcionar semejante garantía. Según otra forma de realización de la presente invención, se hace una provisión para contrarrestar la posibilidad de que se pierda una clave secreta. Esta forma de realización, combinable con cualquiera de las formas de realización anteriormente descritas donde el dispositivo de almacenamiento móvil ejecuta la encriptación o desencriptación del valor privado, se beneficia del hecho de que el usuario generalmente tiene un dispositivo de computación en algún lugar en su hogar. El dispositivo de computación puede ser un ordenador personal, por ejemplo, o un segundo dispositivo de almacenamiento móvil tal como una tableta, por ejemplo. Se hará referencia, por tanto, al dispositivo de computación como un segundo dispositivo de

almacenamiento, donde el segundo dispositivo de almacenamiento es un segundo dispositivo de almacenamiento móvil en el caso donde este sea una tableta. El segundo dispositivo de almacenamiento también tiene medios de comunicaciones con el dispositivo de seguridad virtual, que podría ser una conexión por cable o una conexión inalámbrica. Esta conexión, cuando es inalámbrica, no necesita necesariamente ser de un tipo de proximidad. Según esta forma de realización, donde el dispositivo de almacenamiento móvil tiene que encriptar el valor privado, el dispositivo de seguridad virtual envía una primera parte de la clave secreta al dispositivo de almacenamiento móvil y una segunda parte de la clave secreta al segundo dispositivo de almacenamiento, donde las primeras y segundas partes de la clave son combinables para formar la clave secreta. Ni la primera parte de la clave secreta ni la segunda parte de la clave secreta son suficientes para encriptar o desencriptar el valor privado. Además, no es posible derivar la clave secreta ni solo de la primera parte de la clave secreta ni solo de la segunda parte de la clave secreta. De esta manera, si la clave secreta se pierde alguna vez debido a un error catastrófico, el valor privado se puede todavía recuperar siempre y cuando el dispositivo de almacenamiento móvil y el segundo dispositivo de almacenamiento móvil puedan colaborar entre sí permitiendo que la clave secreta se regenere o se reconstruya de otro modo utilizando las primeras y segundas partes de la clave secreta.

REIVINDICACIONES

1. Método para almacenar de forma segura un valor privado (PV), donde el método utiliza un sistema que comprende:

un dispositivo de almacenamiento móvil (PCD) con un parámetro de identificación (UID), donde el dispositivo de almacenamiento móvil (PCD) comprende una primera interfaz de comunicaciones inalámbricas (WIF1) configurada para establecer una conexión inalámbrica de proximidad local; y
un dispositivo de seguridad virtual (RCV) configurado para llevar a cabo funciones criptográficas, donde el dispositivo de seguridad virtual comprende:

una segunda interfaz de comunicaciones inalámbricas (WIF2) configurada para establecer una conexión inalámbrica de proximidad local;
un módulo de seguridad; y
una memoria segura que comprende una clave secreta (KSI) que corresponde con el parámetro de identificación (UID) del al menos un dispositivo de almacenamiento móvil (PCD), donde dicha clave secreta (KSI) ha sido generada por el dispositivo de seguridad virtual (RCV);

el dispositivo de almacenamiento móvil (PCD) que almacena una clave pública asociada al módulo de seguridad;
donde el método comprende:

establecer un canal de comunicación inalámbrica de proximidad local (SWIF) entre la primera interfaz de comunicaciones inalámbricas (WIF1) y la segunda interfaz de comunicaciones inalámbricas (WIF2);
enviar el parámetro de identificación (UID) del dispositivo de almacenamiento móvil (PCD) al dispositivo de seguridad virtual (RCV) vía el canal de comunicación inalámbrica de proximidad local (SWIF);
enviar el valor privado (PV) del dispositivo de almacenamiento móvil (PCD) al dispositivo de seguridad virtual (RCV) vía el canal de comunicación inalámbrica de proximidad local (SWIF);
encriptar, por el módulo de seguridad, el valor privado (PV) utilizando la clave secreta (KSI) que corresponde con el parámetro de identificación (UID) del dispositivo de almacenamiento móvil (PCD) para dar la versión encriptada del valor privado; y
enviar la versión encriptada del valor privado del dispositivo de seguridad virtual (RCV) para que dicho almacenamiento seguro del valor privado (PV) se haga en el dispositivo de almacenamiento móvil (PCD).

2. Método según la reivindicación 1, que comprende además borrar el valor privado (PV) del dispositivo de almacenamiento móvil (PCD).

3. Método según cualquiera de reivindicaciones 1 o 2, que comprende además generar la clave secreta (KSI) que corresponde con el parámetro de identificación (UID) del dispositivo de almacenamiento móvil (PCD) si ese parámetro de identificación (UID) no está ya almacenado en la memoria segura, donde dicha generación se realiza por el módulo de seguridad.

4. Método según cualquiera de las reivindicaciones precedentes, que comprende además borrar cualquiera, o ambos, del valor privado (PV) y la versión encriptada del valor privado del dispositivo de seguridad virtual (RCV) después de dicho envío de la versión encriptada del valor privado al dispositivo de almacenamiento móvil (PCD).

5. Método según cualquiera de las reivindicaciones precedentes, donde el canal de comunicación inalámbrica de proximidad local (SWIF) es un canal seguro, donde dicho canal se ha asegurado utilizando la clave pública asociada al módulo de seguridad.

6. Método según la reivindicación 5, donde dicha clave pública se recibe desde el dispositivo de seguridad virtual (RCV).

7. Método según la reivindicación 5, donde dicha clave pública se recibe a partir de un servidor de clave pública vía un segundo canal de comunicación diferente del canal de comunicación inalámbrica de proximidad local (SWIF).

8. Método según cualquiera de las reivindicaciones precedentes, donde el canal de comunicación inalámbrica de proximidad local (SWIF) se configura para operar según un estándar de comunicación inalámbrica Bluetooth.

9. Método según cualquiera de las reivindicaciones precedentes, donde el canal de comunicación inalámbrica de proximidad local (SWIF) se configura para operar según un estándar de comunicación inalámbrica de comunicaciones de campo cercano (NFC).

10. Método según cualquiera de las reivindicaciones precedentes, donde el método comprende además una etapa de restaurar el valor personal (PV), donde dicha etapa de restauración comprende:

enviar la versión encriptada del valor privado del dispositivo de almacenamiento móvil (PCD) al dispositivo de seguridad virtual (RCV) vía el canal de comunicación inalámbrica de proximidad local (SWIF);
desencriptar el valor personal por el dispositivo de seguridad virtual (RCV) utilizando la clave secreta (KSI) que corresponde con el dispositivo de almacenamiento móvil (PCD);
retornar el valor personal desencriptado (PV) al dispositivo de almacenamiento móvil (PCD) vía el canal de comunicación inalámbrica de proximidad local (SWIF).

11. Sistema de almacenamiento seguro que comprende un dispositivo de seguridad virtual (RCV) y un dispositivo de almacenamiento móvil (PCD);
donde el dispositivo de almacenamiento móvil (PCD) tiene un parámetro de identificación (UID) y comprende una primera interfaz de comunicaciones inalámbricas (WIF1) configurada para funcionar según un estándar de comunicación inalámbrica de proximidad;
donde el dispositivo de seguridad virtual (RCV) comprende:

una segunda interfaz de comunicaciones inalámbricas (WIF2) configurada para funcionar según el estándar de comunicación inalámbrica de proximidad y para establecer así un canal de comunicación inalámbrica de proximidad local (SWIF) entre el dispositivo de seguridad virtual (RCV) y el dispositivo de almacenamiento móvil (PCD);
una memoria segura que comprende una clave secreta (KSI) que corresponde con el parámetro de identificación (UID) del dispositivo de almacenamiento móvil (PCD), donde dicha clave secreta (KSI) ha sido generada por el dispositivo de seguridad virtual (RCV); y
un módulo de seguridad configurado para:

recibir el valor privado (PV) y el parámetro de identificación (UID) del dispositivo de almacenamiento móvil (PCD) vía el canal de comunicación inalámbrica de proximidad local (SWIF); y
encriptar el valor privado utilizando la clave secreta (KSI) que corresponde con el parámetro de identificación (UID) del dispositivo de almacenamiento móvil (PCD), donde el dispositivo de almacenamiento móvil (PCD) almacena una clave pública asociada al módulo de seguridad;
enviar la versión encriptada del valor privado a dicho dispositivo de almacenamiento móvil (PCD) para el almacenamiento.

12. Sistema de almacenamiento seguro según la reivindicación 11, donde el módulo de seguridad se configura además para generar la clave secreta (KSI) que corresponde con el parámetro de identificación (UID) del dispositivo de almacenamiento móvil (PCD).

13. Sistema de almacenamiento seguro según cualquiera de las reivindicaciones 11 o 12, donde el módulo de seguridad tiene una clave privada correspondiente para asegurar el canal de comunicación inalámbrica de proximidad local (SWIF).

14. Sistema de almacenamiento seguro según cualquiera de las reivindicaciones 11 a 13, donde el dispositivo de almacenamiento móvil (PCD) es un dispositivo de comunicación móvil y el dispositivo de seguridad virtual (RCV) es un dispositivo de recepción de contenido multimedia.

15. Sistema de almacenamiento seguro según cualquiera de las reivindicaciones 11 a 14, donde el estándar de comunicación inalámbrica de proximidad es uno de un estándar Bluetooth o un estándar de Comunicaciones de Campo Cercano (NFC).

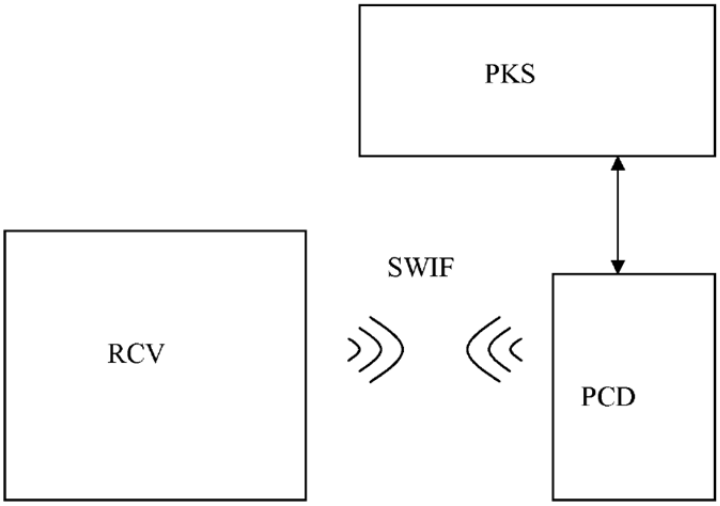

Figura 1

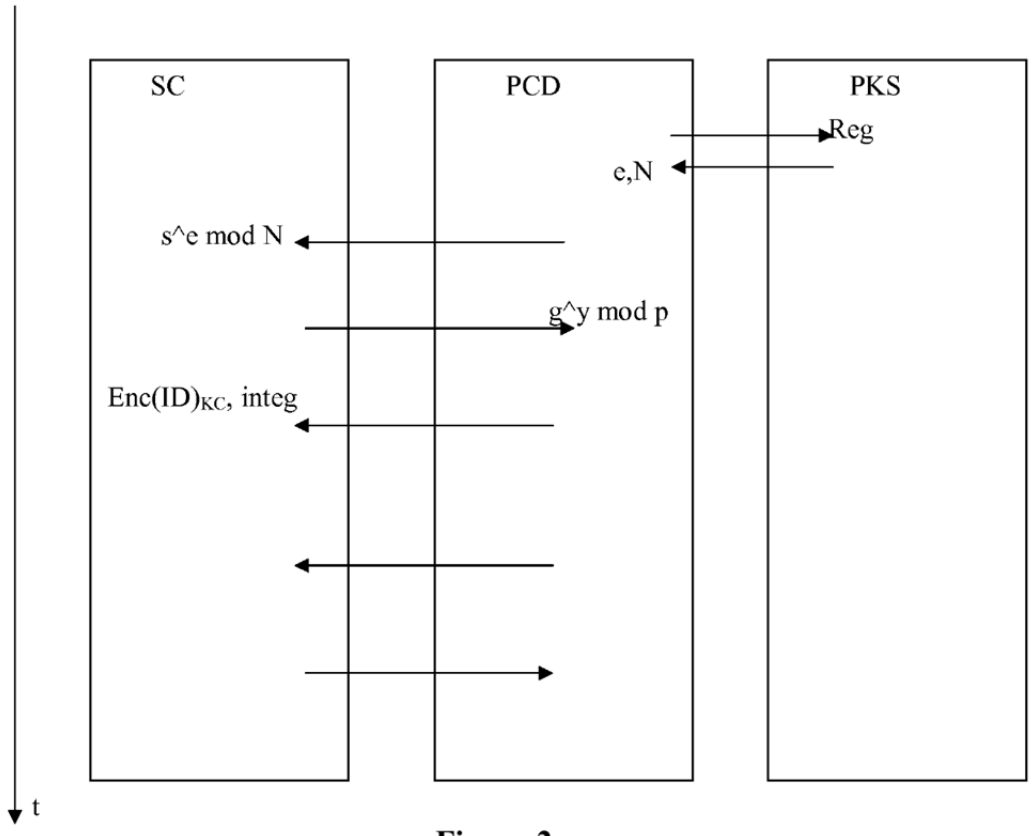

Figura 2