(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 739 896**

(51) Int. CI.:

G06F 21/42 (2013.01)
G06Q 20/32 (2012.01)
G06Q 20/36 (2012.01)
G06Q 20/38 (2012.01)
G07F 7/10 (2006.01)
H04L 29/06 (2006.01)
H04W 12/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.06.2012 E 12170772 (3)**

(97) Fecha y número de publicación de la concesión europea: **01.05.2019 EP 2533172**

(54) Título: **Acceso seguro a datos de un dispositivo**

(30) Prioridad:

06.06.2011 DE 102011050863
01.07.2011 DE 102011051498

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.02.2020

(73) Titular/es:

KOBIL SYSTEMS GMBH (100.0%)
Pfortenring 11
67547 Worms, DE

(72) Inventor/es:

KOYUN, ISMET;
MADLENER, FELIX y
LAUE, RALF

(74) Agente/Representante:

CONTRERAS PÉREZ, Yahel

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Acceso seguro a datos de un dispositivo

Campo de la invención

La invención se refiere a un acceso seguro a datos de un dispositivo, en particular a datos sensibles tales como, por ejemplo, programas informáticos para realizar comunicaciones y/o una clave secreta de un par asimétrico de claves, siendo esta clave secreta para utilizarla en una autenticación, una firma y/o una comunicación cifrada.

Antecedentes de la invención

Hoy en día, a través de Internet se presta toda una gama de servicios con implicaciones de seguridad. Así, por ejemplo, es conocido realizar transacciones bancarias o pagos a través de Internet. Sin embargo, las aplicaciones en línea, tales como la banca en línea o el pago en línea, representan un objetivo para los hackers que desean conocer los datos de seguridad de un usuario y utilizarlos para realizar transacciones en línea en nombre de este último. Por ejemplo, los datos de autenticación del usuario son robados a través de diversas técnicas tales como el phishing o el uso de troyanos, y posteriormente utilizados para realizar pagos.

WO 2004/070587 A1 se refiere al control del descifrado de un programa de aplicación cifrado. Un proveedor del programa de aplicación tiene la posibilidad de controlar el descifrado de la aplicación. La aplicación descifrada se ejecuta en un dispositivo en un entorno seguro, de modo que el propietario del dispositivo no puede acceder a la aplicación de una manera que le permita copiar o manipular la aplicación.

WO 01/06699 A2 divulga un dispositivo cliente en el que se almacena un dispositivo de seguridad personal cifrado. El dispositivo cliente transmite información de autenticación a un servidor de autenticación. Como reacción a la información de autenticación, se puede enviar al dispositivo cliente información de descifrado para el dispositivo de seguridad cifrado procedente de una base de datos de claves.

US 2009/300356 A1 se refiere a un sistema de cifrado para el almacenamiento remoto de datos. El sistema de cifrado incluye un servidor de claves. Un usuario remoto puede solicitar al servidor de claves una clave del servidor de claves. Para ello, se transmite una prueba de autorización de acceso. La prueba de autorización de acceso se valida comparándola con una versión previamente guardada de la prueba de autorización de acceso. A continuación, se selecciona una clave asociada con la prueba de autorización de acceso utilizando una tabla de acceso de claves que se almacena en un módulo de gestión de claves del servidor de claves. La clave seleccionada puede ser enviada al usuario.

US 2007/297610 A1 se refiere a un procedimiento de seguridad de datos basado en una red para un dispositivo móvil. En el dispositivo móvil se almacenan datos cifrados. Si es necesario, el dispositivo móvil solicita una clave de un servidor de claves. Después de la autenticación del usuario del dispositivo móvil, el servidor de claves transfiere la clave al dispositivo móvil. La clave se puede utilizar para descifrar datos cifrados.

Resumen de algunas formas de realización de ejemplo de la presente invención

Aunque los datos de autenticación de un usuario de un dispositivo electrónico (por ejemplo, una clave secreta) estén protegidos en el dispositivo por una contraseña que el usuario debe introducir si desea autenticar estos datos, los delincuentes pueden utilizar un programa maligno (malware) y/o tomar el control del dispositivo para acceder a estos datos de autenticación y luego hacer un uso indebido de los mismos.

Entre otros, el objeto de la presente invención es proporcionar una comunicación segura particular de un dispositivo electrónico.

Este objeto es resuelto por un procedimiento, realizado en un dispositivo electrónico según la reivindicación 1 y por un procedimiento realizado en un servidor según la reivindicación 11. Además, el objeto de la invención es resuelto por un programa informático según la reivindicación 13, un kit de desarrollo de programas informáticos según la reivindicación 14 y un aparato según la reivindicación 15. Se pueden inferir configuraciones ventajosas a partir de las reivindicaciones dependientes.

El procedimiento según la invención, realizado en un dispositivo electrónico, comprende establecer un enlace con un servidor; autenticar al usuario del dispositivo electrónico y/o el dispositivo electrónico en relación con el servidor; y obtener del servidor una primera clave tras una autenticación satisfactoria, en el que la primera clave sirve para descifrar datos cifrados almacenados en el dispositivo electrónico y los datos descifrados están destinados a una comunicación del dispositivo electrónico (por ejemplo, son necesarios, por ejemplo, para una autenticación en el contexto de una comunicación), o en el que la primera clave junto con datos almacenados en el dispositivo electrónico están destinados a una comunicación del dispositivo electrónico.

El procedimiento según la invención, realizado en un servidor, comprende establecer un enlace con un dispositivo electrónico; autenticar al usuario del dispositivo electrónico o el dispositivo electrónico; y suministrar una primera clave tras una autenticación satisfactoria, en el que la primera clave sirve para descifrar datos cifrados almacenados en el dispositivo electrónico y los datos descifrados están destinados a una comunicación del dispositivo electrónico, o en el que la primera clave junto con datos almacenados en el dispositivo electrónico están destinados a una comunicación del dispositivo electrónico. Los datos descifrados incluyen al menos una parte de una segunda clave para autenticar el dispositivo electrónico y/o el usuario del dispositivo electrónico, y/o para cifrar la comunicación del dispositivo electrónico y/o para firmar mensajes del dispositivo electrónico. Además, la segunda clave se ha generado en el dispositivo electrónico en una fase de inicialización.

Se divulga un programa informático según la invención (en lo sucesivo también denominado "software según la invención"), que comprende instrucciones de programa, que hacen que un procesador realice y/o controle las etapas de uno de los procedimientos según la invención, cuando el programa informático es ejecutado en el procesador. En este caso, el procesador puede por ejemplo ser parte del dispositivo electrónico o del servidor, en el cual se realiza el correspondiente procedimiento según la invención. El programa informático puede ser al menos en parte software y/o firmware de un procesador.

El kit de desarrollo de programas informáticos comprende unos módulos de programas informáticos para crear un programa informático de acuerdo con la invención.

En el dispositivo de almacenamiento de datos se almacena un programa informático según la invención o un kit de desarrollo de programas informáticos según la invención. El dispositivo de almacenamiento de datos puede ser, por ejemplo, un medio de almacenamiento legible informáticamente que contiene un programa informático según la invención y/o un kit de desarrollo de programas informáticos según la invención y puede, por ejemplo, estar integrado como un medio de almacenamiento magnético, eléctrico, electromagnético, óptico y/u otro tipo de medio de almacenamiento.

El aparato comprende medios para realizar al menos uno de los procedimientos según la invención. El aparato según la invención es, por ejemplo, el dispositivo electrónico en el que se realiza el correspondiente procedimiento según la invención, o el servidor, en el que se realiza el correspondiente procedimiento según la invención. Dichos medios pueden comprender, por ejemplo, un procesador.

Un sistema según la invención puede comprender un dispositivo electrónico que tiene unos medios para realizar el correspondiente procedimiento según la invención y el servidor.

A continuación se describen formas de realización de ejemplo de la presente invención, que se centran en características de ejemplo adicionales de los procedimientos según la invención, del programa informático según la invención, del kit de desarrollo de programas informáticos según la invención, del dispositivo de almacenamiento de datos según la invención, del aparato según la invención y del sistema según la invención. En particular, debería considerarse que se ha hecho también, mediante la descripción de una etapa de procedimiento adicional de un procedimiento según la invención, una divulgación de medios para realizar la etapa de procedimiento del correspondiente aparato según la invención, de un correspondiente módulo de programa informático de los kits de desarrollo de programas informáticos según la invención y de una correspondiente instrucción de programa del correspondiente programa informático según la invención, que causan que un procesador realice la etapa de procedimiento, cuando el programa informático es ejecutado en el procesador. Lo mismo aplicará a la divulgación de un medio para realizar una etapa de procedimiento o una instrucción de programa, por ejemplo se considerará que la divulgación de un medio para realizar una etapa de procedimiento es una divulgación del correspondiente procedimiento y de una instrucción de programa correspondiente.

Un dispositivo electrónico es, por ejemplo, un aparato que está configurado para el procesamiento de datos con la ayuda de un procesador, por ejemplo, un dispositivo de procesamiento de datos tal como un dispositivo informático, un cliente ligero, un servidor, un dispositivo informático portátil, un asistente digital personal, un teléfono móvil y/o cualquier otro dispositivo electrónico que disponga de un procesador. Un procesador también abarca, entre otras cosas, unidades de control, microprocesadores, unidades de micro control tales como microcontroladores, procesadores de señales digitales (DSP), circuitos integrados de aplicaciones específicas (ASIC) o matrices de puertas programables de campo (FPGA).

Por ejemplo, un programa informático almacenado en un medio legible informáticamente según la invención podría ser ejecutado por un procesador de un dispositivo electrónico y hacer que el dispositivo electrónico realice el correspondiente procedimiento según la invención en el dispositivo electrónico.

El enlace entre el dispositivo electrónico y el servidor es, por ejemplo, un enlace de datos cableado y/o inalámbrico. Por ejemplo, el enlace es, al menos en parte, un enlace de datos de red (por ejemplo, un enlace de datos Ethernet,

Fast Ethernet, Gigabit Ethernet, DSL (Línea Digital de Suscripción) y/o un enlace de datos WLAN) y/o, al menos en parte, un enlace de datos de telefonía móvil (por ejemplo, un enlace de datos GSM (sistema Global para Comunicaciones Móviles), UMTS (sistema Universal de Telecomunicaciones Móviles), GPRS (servicio General de Radio comunicaciones por Paquetes), HSDPA (Acceso por Paquetes de Enlace Descendente de Alta Velocidad), HSUPA (Acceso por Paquetes de Enlace Ascendente de Alta Velocidad) y/o un enlace de Datos LTE (Evolución a Largo Plazo). Por ejemplo, el enlace de datos es creado a través de una red de área local (LAN), una red de área extendida (WAN) y/o Internet. Por ejemplo, el dispositivo electrónico comprende al menos una interfaz de datos para establecer un enlace de datos con el servidor y/o el servidor comprende al menos una interfaz de datos para establecer un enlace de datos con el dispositivo electrónico.

Sólo si el servidor autentica satisfactoriamente al usuario (y/o al dispositivo electrónico), el servidor suministra la primera clave de salida, por ejemplo, enviada a través del enlace al dispositivo electrónico. Sólo si el usuario (y/o el dispositivo electrónico) se auto autentica satisfactoriamente en relación con el servidor, la primera clave es recibida por el dispositivo electrónico, por ejemplo, a través del enlace con el servidor.

La autenticación del usuario del dispositivo electrónico (y/o del dispositivo electrónico) en relación con el servidor tiene lugar, por ejemplo, mediante el suministro de información de autenticación del usuario por parte del dispositivo electrónico al servidor, por ejemplo, a través del enlace con el servidor. La autenticación del usuario (y/o de los dispositivos electrónicos) en el servidor tiene lugar, por ejemplo, comprobando la autenticación del usuario del dispositivo electrónico obtenida por el servidor, por ejemplo, recibida a través del enlace con el dispositivo electrónico.

La información de autenticación del usuario puede ser, por ejemplo, una contraseña, una firma digital y/o un certificado de software, tal como por ejemplo un certificado RSA (Rivest Shamir Adleman). La información de autenticación del usuario se obtiene, por ejemplo, en el dispositivo electrónico a través de un input de usuario y/o a través de un dispositivo de autenticación de usuario conectado con el dispositivo electrónico. La autenticación del usuario (y/o del dispositivo electrónico) tiene lugar, por ejemplo, en forma de una denominada autenticación de dos factores. La información de autenticación del usuario también puede contener o incluir información biométrica del usuario. Por ejemplo, una huella, una muestra de voz o un escaneado del iris pueden servir como información de autenticación del usuario.

Es preferible que la información de autenticación del usuario no esté almacenada (o al menos no de forma permanente) en el dispositivo electrónico, ya que se comprueba exclusivamente en el servidor.

La información de autenticación del usuario está, por ejemplo, relacionada con el usuario y sirve para la autenticación de un usuario en particular o de un grupo de usuarios por parte del servidor. Por ejemplo, durante una fase de inicialización que se realizará una vez para cada usuario, se define en el servidor la respectiva información de autenticación del usuario (por ejemplo, diferente para cada usuario) individual. En la fase de inicialización, el usuario realiza una auto autenticación, por ejemplo, mediante una contraseña de activación de una sola vez para el servidor. Por ejemplo, el usuario recibe una contraseña de activación de una sola vez a través de un canal separado, tal como por correo.

Comprobando la información de autenticación suministrada por el dispositivo electrónico al servidor frente a la información de autenticación del usuario definida en la fase de inicialización, el usuario (y/o el dispositivo electrónico) puede, por ejemplo, ser autenticado en el servidor. El servidor puede, por ejemplo, contar los intentos de autenticación fallidos de un usuario de los dispositivos electrónicos (y/o del dispositivo electrónico) en relación con el servidor. Por ejemplo, si el usuario excede un cierto número (por ejemplo, predefinido) de intentos de autenticación fallidos por parte de un usuario (y/o del dispositivo electrónico), el usuario (y/o el dispositivo) puede ser bloqueado por el servidor. De esta manera, por ejemplo, se puede evitar una autenticación satisfactoria de un atacante con respecto al servidor mediante simple ensayo y error (el llamado procedimiento de fuerza bruta).

Para la autenticación del usuario y/o del dispositivo electrónico, además de la información de autenticación del usuario (por ejemplo, un PIN), se puede poner a disposición del servidor (y también recibida y comprobada por este último) información adicional, por ejemplo, información sobre un programa que el usuario utiliza para la autenticación en relación con el servidor (este programa puede ser, por ejemplo, el programa según la invención o parte del mismo). La información se puede referir, por ejemplo, a una identificación (por ejemplo, en forma de un número de identificación único) del programa y/o un estado del programa. En base a esta información, el servidor puede, por ejemplo, comprobar si el programa está registrado (por ejemplo, en el servidor) para el dispositivo electrónico (por ejemplo, para un dispositivo electrónico específico y no para otro dispositivo electrónico), si el programa sigue estando en el estado original (o en un estado que es el resultado del estado original y simplemente actualizaciones oficiales) y/o si la versión del programa es correcta o si es necesaria una actualización. Sólo entonces, por ejemplo, se puede considerar que la autenticación del usuario y/o del dispositivo electrónico ha sido satisfactoria y se ha suministrado la primera clave, si se ha establecido que la información de autenticación del usuario es correcta, el

programa está registrado para el dispositivo electrónico, el programa se encuentra en su estado original (posiblemente incluyendo actualizaciones oficiales) y/o se encuentra en la versión correcta.

La primera clave es, por ejemplo, una clave individual para cada usuario (y/o el dispositivo electrónico). La primera clave es definida, por ejemplo, para cada usuario (y/o cada dispositivo electrónico) en una fase de inicialización que se realiza una sola vez y se guarda de forma permanente en el servidor. La primera clave preferiblemente no se almacena de forma permanente en el dispositivo electrónico y después de cada realización del procedimiento según la invención, el dispositivo electrónico elimina la primera clave del dispositivo electrónico. A modo de ejemplo, la clave tiene una longitud de 128 bits, 192 bits o 256 bits. Esta es una ventaja, entre otras cosas, con el fin de que el usuario pueda utilizar una contraseña sencilla para autenticarse en relación con el servidor, pero al mismo tiempo permitir que la comunicación del dispositivo electrónico esté protegida por una contraseña segura.

La comunicación para la cual están destinados los datos descifrados es, por ejemplo, una comunicación particular (por ejemplo, una comunicación predefinida) (por ejemplo, un tipo (por ejemplo, predefinido) de comunicación particular), y/o una comunicación con una o más partes de comunicación particulares asociadas (por ejemplo, servidores).

La comunicación referida, por ejemplo, no es la única comunicación que puede realizar el dispositivo electrónico. De este modo, son posibles y/o pueden ser controladas otras comunicaciones sin la parte del software contenida en los datos cifrados.

La comunicación referida es, por ejemplo, una comunicación que requiere una autenticación del dispositivo electrónico y/o una autenticación de un usuario del dispositivo electrónico (y/o del dispositivo electrónico). Los datos descifrados pueden entonces, por ejemplo, contener al menos parte de la información necesaria para esta autenticación (por ejemplo, la segunda clave) o ser necesarios para el uso de (por ejemplo, el acceso a) al menos parte de dicha información. La autenticación puede ser, por ejemplo, una autenticación (por ejemplo, una autenticación en el lado del cliente que requiere, entre otras cosas, una firma de datos (por ejemplo, una petición enviada por el servidor al cliente) con una clave secreta del cliente) en el contexto de un enlace seguro, por ejemplo, un enlace de capa de puertos seguros (SSL: Secure Socket Layer) / seguridad de la capa de transporte (TLS: Transport Layer security) de acuerdo con el documento de solicitud de comentarios (RFC: Request for Comments) 5246, o un enlace seguro de acuerdo con un protocolo propietario. La autenticación puede, por ejemplo, incluir adicional o alternativamente la firma de un mensaje (por ejemplo, por medio del cifrado de un valor hash del mensaje), por ejemplo, con la segunda clave. El mensaje puede ser, por ejemplo, una confirmación de un proceso de inicio de sesión o transacción que el usuario realiza en el servidor de un proveedor de servicios (por ejemplo, siendo dicho servidor diferente o igual al servidor desde el que se recibe la clave), para el que se muestra información al usuario en el dispositivo electrónico y que éste último puede confirmar o rechazar. El mensaje firmado es entonces, por ejemplo, transmitido al servidor y verificado y/o archivado en el mismo.

Por ejemplo, el dispositivo electrónico puede sólo realizar la comunicación con la ayuda de la primera clave, por ejemplo, una comunicación bancaria en línea. Esto es ventajoso, entre otras cosas, porque un atacante, incluso si está en posesión del dispositivo electrónico, debe realizar una auto autenticación satisfactoria en relación con el servidor con el fin de poder utilizar la comunicación del dispositivo electrónico.

La comunicación es, por ejemplo, una comunicación segura con un servidor, por ejemplo, con un servidor de un servicio de comunicación de banca en línea. Este servidor puede corresponder al servidor desde el que se obtiene la primera clave o puede ser otro servidor. La comunicación segura sirve, por ejemplo, para el intercambio de información sobre transacciones bancarias en línea y/o números de transacción (TAN) para la confirmación de transacciones bancarias en línea a través de un canal seguro, o para la confirmación o rechazo de procedimientos de inicio de sesión y/o transacción que realiza el usuario del dispositivo electrónico en un servidor del proveedor de servicios, a través de un canal seguro, en particular a través de un canal seguro que es independiente del canal a través del cual el usuario del dispositivo electrónico realiza los procedimientos de inicio de sesión y/o transacción en el servidor del proveedor de servicios.

Por ejemplo, la primera clave sirve para descifrar datos cifrados almacenados en el dispositivo electrónico, en el que los datos descifrados están destinados a una comunicación del dispositivo electrónico. Por ejemplo, los datos son cifrados con la primera clave, por ejemplo, de forma asimétrica o simétrica. Por ejemplo, los datos son cifrados según el procedimiento de cifrado Estándar de Cifrado Avanzado (AES: Advanced Encryption Standard). La primera clave es, por ejemplo, una clave según el estándar AES.

Por ejemplo, los datos descifrados comprenden al menos una parte (o todos los componentes) de un programa informático (por ejemplo, una aplicación que ha sido descargada al dispositivo electrónico), que permite y/o controla al menos parcialmente la comunicación del dispositivo electrónico (por ejemplo, con un servidor de banca en línea). El código de programa ejecutable del software puede entonces, por ejemplo, ser almacenado de forma cifrada en

una memoria (por ejemplo, una memoria de programas tal como una memoria flash) del dispositivo electrónico y sólo ser ejecutable una vez que ha sido descifrado. Para su ejecución puede ser copiado (en forma descifrada), por ejemplo, a otra memoria del dispositivo electrónico o a otra área de memoria de la misma memoria, en la que se almacenó de forma cifrada. A efectos de ejecución, el código de programa ejecutable puede ser descifrado en una memoria volátil, por ejemplo, una memoria RAM (a modo de ejemplo, una memoria de trabajo). Una vez ejecutado, por ejemplo, puede ser borrado de la memoria volátil o sobrescrito. De esta manera se puede evitar de forma ventajosa que el programa descifrado permanezca en forma descifrada permanentemente.

Adicional o alternativamente a la parte del software, los datos descifrados contienen al menos una segunda clave (o una parte de la misma), con la cual (o en base a la cual) el usuario (y/o el dispositivo electrónico) puede, por ejemplo, realizar la auto autenticación en relación con un servicio de comunicación, por ejemplo, un servicio de comunicación de banca en línea, o un servidor, por ejemplo, el servidor del cual se obtuvo la primera clave. La segunda clave se puede utilizar, por ejemplo, para una autenticación en el lado del cliente cuando se establece un enlace seguro (por ejemplo, un enlace SSL o TLS) con un servidor (por ejemplo, el servidor del cual se obtiene la primera clave) y/o para la firma de mensajes (por ejemplo, confirmaciones de inicio de sesión y/o procesos de transacción). Con la autenticación en el lado del cliente, el dispositivo electrónico puede, por ejemplo, firmar una petición proporcionada por el servidor, que a su vez puede ser comprobada con una clave asociada con la segunda clave en el servidor (por ejemplo, mediante descifrado del valor hash de la petición contenida en la firma, recálculo del valor hash de la petición en el servidor y comparación de los valores hash).

Adicional o alternativamente a la parte del software, los datos descifrados también pueden contener simplemente una parte de una segunda clave, que sólo puede ser utilizada para la autenticación conjuntamente con otra parte de la segunda clave (que por ejemplo es guardada en el servidor, por ejemplo en forma cifrada o no cifrada). Las dos partes pueden constituir, por ejemplo, una clave distribuida, por ejemplo, una clave RSA privada distribuida.

Si los datos descifrados comprenden al menos parte del programa informático o software, que permite y/o controla al menos parcialmente una comunicación del dispositivo electrónico, y la segunda clave (o una parte de la misma), la segunda clave (o una parte de la misma) puede, por ejemplo, estar contenida en la parte del programa informático y/o estar asociada con esta parte del programa informático o software. En el primer caso, se cifra entonces la segunda clave (o parte de la misma) mediante, por ejemplo, el cifrado de la parte del software; en el segundo caso, por ejemplo, se cifra la segunda clave (o una parte de la misma) junto con la parte del software o por separado de la misma. La segunda clave (o parte de la misma) puede, por ejemplo, servir al menos para la autenticación parcial en relación con la comunicación, que es al menos parcialmente habilitada y/o al menos parcialmente controlada a través de la parte del software.

La segunda clave es, por ejemplo, una clave secreta de un par asimétrico de claves que sirve para la autenticación del usuario y/o del dispositivo electrónico (por ejemplo, en un servicio de comunicación, por ejemplo, un servidor del servicio de comunicación, o en un servidor, por ejemplo, el servidor del cual se obtiene la primera clave). Un ejemplo del procedimiento de cifrado asimétrico es el procedimiento Rivest-Shamir-Adleman (RSA). Por ejemplo, la segunda clave es una clave RSA.

La segunda clave se puede almacenar, por ejemplo, en una primera memoria del dispositivo electrónico, mientras que otras claves secretas del dispositivo electrónico se almacenan en una segunda memoria. La segunda y primera memorias pueden ser, por ejemplo, memorias diferentes. La segunda memoria puede, por ejemplo, estar ya disponible en el mismo momento de la entrega del dispositivo electrónico, mientras que la primera memoria, por ejemplo, sólo es reservada o almacenada en el dispositivo electrónico, por ejemplo, tras la instalación de un software, con el que se realiza la autenticación en el servidor (por ejemplo, el programa informático según la invención). La primera memoria está, por ejemplo, totalmente cifrada con la primera clave y sólo se puede descifrar con la misma.

Los datos descifrados pueden, por ejemplo, contener al menos una parte de un software y/o información que es necesaria para obtener información de autenticación almacenada en el servidor (tal como, por ejemplo, una clave o una parte de la misma, por ejemplo, la segunda clave descrita anteriormente, o información derivada de esta clave). La información de autenticación puede, por ejemplo, servir para la autenticación al menos parcial del dispositivo electrónico y/o de un usuario del dispositivo electrónico en la comunicación del dispositivo electrónico. La información de autenticación (por ejemplo, una clave secreta o una parte de la misma) se puede almacenar, por ejemplo, de forma cifrada en el servidor y la información contenida en los datos descifrados puede, por ejemplo, ser una clave para descifrar esta información de autenticación. Si la información de autenticación forma parte de una clave secreta, la otra parte se puede almacenar, por ejemplo, en el dispositivo; puede, por ejemplo, formar parte de los datos descifrados.

Los datos descifrados pueden, por ejemplo, contener al menos parte de un programa informático y/o información que es necesaria para el uso de la información de autenticación a la que puede acceder un aparato (inalámbrico o

cableado) que puede conectarse con el dispositivo electrónico (por ejemplo, un lector de tarjetas inteligentes o un medio de almacenamiento).

La información de autenticación (tal como, por ejemplo, una clave o una parte de la misma, por ejemplo, la segunda clave descrita anteriormente o una parte de la misma, o información derivada de esta clave) puede servir, por ejemplo, para la autenticación del dispositivo electrónico y/o de un usuario del dispositivo electrónico en la comunicación del dispositivo electrónico. Por ejemplo, es posible que la información de autenticación no se pueda leer del aparato. El uso de la información de autenticación puede comprender, por ejemplo, realizar operaciones con datos (por ejemplo, una firma o un cifrado) utilizando la información de autenticación y obteniendo los resultados.

La información contenida en los datos que han sido descifrados (con la primera clave) puede ser, por ejemplo, información (por ejemplo, una contraseña o un PIN del aparato o un medio al que el aparato puede acceder), que es necesaria para uso de la información de autenticación.

La información puede, por ejemplo, haber sido introducida por un usuario del dispositivo electrónico (por ejemplo, una sola vez) y luego (posiblemente con otros datos) haber sido cifrada con la primera clave, con el fin de obtener los datos cifrados.

La información contenida en los datos que se han descifrado (con la primera clave) puede ser, por ejemplo, una clave con la que se cifra la información almacenada en el servidor (por ejemplo, una contraseña, un PIN del aparato o un medio al que el aparato puede acceder, o parte de la contraseña/PIN), que es necesaria para el uso de la información de autenticación. A modo de ejemplo, el servidor puede almacenar un PIN en forma cifrada, en el que la clave para descifrar el PIN está contenida en los datos que se descifran (con la primera clave) y el PIN es necesario para el uso de la información de autenticación del aparato (por ejemplo, porque está involucrado el PIN de una tarjeta inteligente (smartcard) a la que el aparato puede acceder cuando está presente el PIN). El servidor también puede almacenar sólo una parte de este PIN en forma cifrada, en el que la otra parte, por ejemplo, se debe introducir (por ejemplo, sin cifrar) en el dispositivo electrónico o en el aparato.

Si los datos descifrados contienen al menos una parte de un programa informático, que es necesario para el uso de la información de autenticación, al que puede acceder un aparato que puede conectarse al dispositivo electrónico, el programa informático o software puede contener, por ejemplo, información que es necesaria para la autenticación en relación con el aparato. Esta información puede, por ejemplo, ser diferente de un PIN (por ejemplo, un PIN de tarjeta inteligente) asociado con la información de autenticación, al que el aparato puede acceder y, por ejemplo, ser específico sólo para el aparato (por ejemplo, un lector de tarjeta inteligente).

Por ejemplo, la primera clave junto con los datos almacenados en el dispositivo electrónico está destinada a la comunicación del dispositivo electrónico. Por ejemplo, la primera clave junto con una segunda clave almacenada en el dispositivo electrónico constituye una tercera clave con la que el usuario (y/o el dispositivo electrónico) puede realizar una auto autenticación en relación con un servicio de comunicación, por ejemplo, un servicio de comunicación de banca en línea, o un servidor. La tercera clave es, por ejemplo, una clave secreta de un par asimétrico de claves que sirve para la autenticación del usuario (y/o del dispositivo electrónico) en relación con el servicio de comunicación (o un servidor del servicio de comunicación). Por ejemplo, la tercera clave es una clave RSA. De esta manera, el uso de la comunicación sólo es posible si se conocen tanto la primera clave almacenada en el servidor como la segunda clave almacenada en el dispositivo electrónico.

Según una forma de realización de ejemplo de la invención, la autenticación del usuario del dispositivo electrónico y/o del dispositivo electrónico en relación con el servidor comprende obtener información de autenticación del usuario en el dispositivo electrónico; y la transmisión de la información de autenticación del usuario al servidor.

Según una forma de realización de ejemplo de la invención, la información de autenticación del usuario se obtiene de un aparato de autenticación de usuarios en el dispositivo electrónico.

El aparato de autenticación de usuarios es, por ejemplo, un lector de tarjetas, por ejemplo, un lector de tarjetas de la clase de seguridad 1, 2, 3 o 4 según las especificaciones del Zentral Kreditausschuss (Comité Central de Crédito Alemán - ZKA). Preferiblemente un lector de tarjetas de la clase de seguridad 3 o 4. Por ejemplo, una tarjeta inteligente puede ser configurada de tal manera que permita que la información de autenticación del usuario sólo sea leída por el lector de tarjetas y la suministre al dispositivo electrónico conectado al lector de tarjetas si el usuario ha introducido una contraseña (por ejemplo, en el dispositivo electrónico o en el lector de tarjetas) asignada a la información de autenticación del usuario (autenticación de dos factores), por ejemplo, la información de autenticación del usuario podría ser cifrada y descifrada con la contraseña por medio de la tarjeta inteligente (por ejemplo, dentro de la tarjeta inteligente). La tarjeta inteligente es, por ejemplo, una tarjeta de identificación digital.

El aparato de autenticación de usuarios se conecta, por ejemplo, de forma inalámbrica o por cable con el dispositivo electrónico, por ejemplo, a través de una interfaz de datos Bluetooth y/o una interfaz de datos USB.

De acuerdo con una forma de realización de ejemplo de la invención, los procedimientos según la invención también comprenden, en una fase de inicialización, el registro del usuario (y/o del dispositivo electrónico) y/o la información de autenticación del usuario en el servidor.

Según una forma de realización de ejemplo de la invención, el procedimiento según la invención realizado en el dispositivo electrónico comprende descifrar los datos cifrados almacenados en el dispositivo electrónico con la primera clave; y usar los datos descifrados para la comunicación.

Según una forma de realización de ejemplo de la invención, el procedimiento según la invención, realizado en el dispositivo electrónico comprende cifrar los datos con la primera clave; y almacenar los datos cifrados en el dispositivo electrónico. Si la primera clave se ha generado individualmente para un usuario del dispositivo electrónico (y/o para el dispositivo electrónico), por medio del cifrado de los datos (por ejemplo, un programa informático para la comunicación del dispositivo electrónico y/o de la segunda clave) también se consigue automáticamente una individualización de los datos cifrados en el dispositivo electrónico. De esta manera se puede conseguir, en primer lugar, dificultar el análisis (delictivo) del cifrado, ya que – incluso cuando se asumen los mismos datos en varios dispositivos electrónicos, en los que, sin embargo, los datos son codificados en cada dispositivo electrónico con diferentes primeras claves – habría que recurrir a una serie de dispositivos electrónicos y, en segundo lugar, que incluso con el descubrimiento (delictivo) o el cálculo (delictivo) de la primera clave de un dispositivo electrónico, sólo son accesibles/usables los datos de este dispositivo electrónico, pero no los datos de otros dispositivos electrónicos.

Según la invención, los datos almacenados en el dispositivo electrónico comprenden al menos una segunda clave (o una parte de la segunda clave) para la autenticación del usuario del dispositivo electrónico y/o del dispositivo electrónico y/o para el cifrado de la comunicación del dispositivo electrónico y/o para la firma de mensajes del dispositivo electrónico. La autenticación del usuario y/o del dispositivo puede ser necesaria, por ejemplo, para establecer un enlace seguro (por ejemplo, un enlace SSL o TLS) entre el dispositivo y un servidor (por ejemplo, un servidor de un proveedor de servicios en línea (por ejemplo, para la banca en línea) o el servidor del cual se obtiene la primera clave), por ejemplo, para la autenticación en el lado del cliente. A modo de ejemplo, la segunda clave se utiliza para firmar una petición recibida procedente del servidor (o, por ejemplo, información que es generada por el dispositivo electrónico y/o el servidor, en el que esta información, por ejemplo, depende de la sesión en la que se produce la autenticación), en el que la firma puede entonces ser verificada en el servidor con una clave asociada con la segunda clave. El enlace seguro se puede basar, por ejemplo, en un cifrado simétrico en base a una clave de sesión, en el que la clave de sesión, o información, de la que depende la clave de sesión, es cifrada con, por ejemplo, una clave pública del servidor a través del dispositivo electrónico y, a continuación, puede ser descifrada por el servidor con la clave privada asociada, por medio de la cual, por ejemplo, se puede conseguir la autenticación en el lado del servidor. La clave de sesión se puede utilizar adicional o alternativamente para o como base para una protección MAC (Message Authentication Code: Código de Autenticación de Mensaje) del enlace seguro. A modo de ejemplo, hay una primera clave de sesión para el cifrado y una segunda clave de sesión para la protección MAC. Sin embargo, ambas claves de sesión se pueden derivar de la misma clave de sesión, por ejemplo, mediante la creación de un valor hash.

Mensajes del dispositivo electrónico (por ejemplo, procedimientos de inicio de sesión y/o transacción confirmados o rechazados por el dispositivo electrónico, por ejemplo, en un servidor de un proveedor de servicios en línea tal como, por ejemplo, un banco), pueden ser firmados con la segunda clave (por ejemplo, mediante la creación de un valor hash y el cifrado del valor hash), por ejemplo, también si estos procedimientos de inicio de sesión y/o transacción confirmados o rechazados son enviados a través de un enlace seguro, ya que los procedimientos de inicio de sesión y/o transacción confirmados o rechazados firmados pueden ser archivados a efectos de prueba en forma firmada. Si la segunda clave se utiliza para la autenticación en relación con el servidor desde el que se recibió la primera clave (y en el que ya se ha realizado la autenticación del usuario y/o del dispositivo utilizando la información de autenticación del usuario), se consigue el efecto ventajoso de que el usuario puede habilitar la segunda clave, que es, por ejemplo, una clave RSA más larga, a través de, por ejemplo, información de autenticación del usuario relativamente corta (por ejemplo, un PIN de cuatro, cinco o seis dígitos) y, por ejemplo, ya no tiene que preocuparse por la autenticación en base a la segunda clave (por ejemplo, cuando se establece un enlace seguro o cuando se firman mensajes), ya que esto, por ejemplo, se produce automáticamente. Otro efecto ventajoso es que antes de la habilitación de la segunda clave por parte del servidor no sólo se comprueba el PIN del usuario, sino también, opcionalmente, otras características del dispositivo electrónico y/o del software con las que el usuario se autentica en relación con el servidor, por ejemplo, si el software se encuentra todavía en el estado original (o en un estado que es el resultado del estado original y de meras actualizaciones oficiales), si la versión del software está actualizada, y/o si el software está registrado para el dispositivo electrónico.

Según la invención, el procedimiento según la invención realizado en el dispositivo electrónico también comprende en una fase de inicialización generar la segunda clave en el dispositivo electrónico. La segunda clave puede ser, por ejemplo, una clave secreta (o privada) de un par asimétrico de claves (por ejemplo, un par de claves RSA). En este caso, por ejemplo, se puede generar una clave pública correspondiente a la segunda clave que, por ejemplo, es suministrada por el dispositivo electrónico a, por ejemplo, el servidor del cual se obtiene la primera clave.

El procedimiento según la invención, realizado en el dispositivo electrónico, puede incluir además en la fase de inicialización suministrar una clave pública asociada con la segunda clave al servidor para permitir al servidor generar un certificado (por ejemplo, un certificado de clave pública) basado en la clave pública firmada con una clave del servidor. El certificado puede, por ejemplo, incluir la clave pública y la firma de una representación (por ejemplo, un valor hash) de la misma. La firma se genera con una clave del servidor, por ejemplo, una clave privada del servidor. La clave privada del servidor puede, por ejemplo, constituir una autoridad de certificación (por ejemplo, ser la clave secreta (clave ROOT) de la autoridad de certificación) o puede estar asociada con un certificado (que, por ejemplo, comprende su clave pública asociada) que ha sido firmado con la clave secreta (clave ROOT) de una autoridad de certificación. El certificado generado por el servidor puede, por ejemplo, ser comprobado con un certificado (por ejemplo, un certificado de clave pública) que corresponde a la clave privada del servidor y que, por ejemplo, ha sido firmado con la clave secreta de una ROOT de la autoridad de certificación.

El certificado generado por el servidor puede, por ejemplo, ser recibido por el dispositivo electrónico procedente del servidor. Por ejemplo, se puede entonces proporcionar a una entidad (por ejemplo, a un proveedor de servicios en línea como, por ejemplo, un banco) para que pueda autenticar al menos a uno de los usuarios del dispositivo electrónico y al dispositivo electrónico. La entidad puede entonces, por ejemplo, comprobar el certificado recibido procedente del dispositivo electrónico en base al certificado del servidor (en el que la entidad, por ejemplo, confía en el certificado del servidor o puede verificarlo en base a otro certificado).

Alternativamente, el certificado generado por el servidor puede ser proporcionado a la entidad por parte del servidor.

Según una forma de realización de ejemplo de la invención, la primera clave es una clave que es individual para el usuario, en el que la primera clave puede ser generada por el servidor durante la fase de inicialización (así, por ejemplo, es generada). En particular, la clave puede ser generada por el servidor en una fase de inicialización de forma aleatoria (así, por ejemplo, es generada aleatoriamente), de este modo, por ejemplo, según una especificación para la generación de una clave aleatoria (por ejemplo, por medio de un registro de desplazamiento).

De acuerdo con una forma de realización de ejemplo de la invención, el enlace con el servidor y/o la comunicación del dispositivo electrónico es securizado. En particular, el enlace y/o la comunicación es/son seguros según el protocolo de capa de puertos seguros (SSL: Secure Socket Layer) y/o el protocolo de seguridad de la capa de transporte (TLS: Transport Layer security).

Según una forma de realización de ejemplo de la invención, la comunicación del dispositivo electrónico es una comunicación bancaria en línea. Alternativamente, la comunicación del dispositivo electrónico puede ser una comunicación del dispositivo electrónico con el servidor, del cual se obtiene la primera clave. En el contexto de esta comunicación, por ejemplo, el servidor puede enviar información sobre procedimientos de inicio de sesión o de transacción que, por ejemplo, se realizan en relación con el uso de un servicio en línea (por ejemplo, la banca en línea), al dispositivo electrónico y mostrársela al usuario para que el usuario pueda confirmar o rechazar los procedimientos de inicio de sesión o de transacción. En el contexto de la comunicación, se puede enviar entonces información sobre la confirmación o el rechazo por parte del usuario al servidor (por ejemplo, firmada con la segunda clave), que a continuación, por ejemplo, envía información sobre la confirmación o el rechazo del usuario a otro servidor, por ejemplo, un servidor en el que se ha realizado el procedimiento de inicio de sesión y/o transacción.

Según una forma de realización de ejemplo de la invención, la comunicación se produce entre el dispositivo electrónico y el servidor y sirve para la autenticación – en particular, autenticación fuera de banda (por ejemplo, adicional) – del usuario para los procedimientos de inicio de sesión y/o transacción, que son realizados por el usuario del dispositivo electrónico con el dispositivo electrónico u otro dispositivo en el servidor de un proveedor de servicios. A modo de ejemplo, el servidor del proveedor de servicios (por ejemplo, un servidor de banca en línea) puede enviar una consulta al servidor del cual se obtiene la primera clave, para obtener la confirmación del procedimiento de inicio de sesión y/o transacción. El servidor (del cual se obtiene la primera clave) puede en este momento enviar al dispositivo electrónico información relativa al procedimiento de inicio de sesión y/o transacción y pedir al usuario confirmación o rechazo. La consulta de confirmación o rechazo se puede mostrar, por ejemplo, en una pantalla proporcionada por el software que el usuario utiliza para la auto autenticación en el servidor, que difiere de una pantalla también proporcionada por el software o al menos controlada por el mismo, en el que se muestra información procedente de una aplicación (por ejemplo, una aplicación de navegador), a través de la cual el usuario realiza los procedimientos de inicio de sesión y/o transacción. La información relativa a la confirmación o rechazo del usuario puede entonces, por ejemplo, ser devuelta firmada con la segunda clave al servidor (del cual se obtiene la

primera clave), que a su vez devuelve la correspondiente información al servidor del proveedor de servicios que ha realizado la consulta. De este modo, en un canal de comunicación entre el servidor, del cual se obtiene la primera clave, y el dispositivo electrónico que es independiente de la comunicación del dispositivo electrónico (u otro dispositivo, por ejemplo, un dispositivo informático) con el servidor del proveedor de servicios (es decir, un canal fuera de banda), es posible, por lo tanto, una autenticación adicional (una autenticación fuera de banda) del usuario en el contexto del procedimiento de inicio de sesión y/o transacción. En lugar de la confirmación del procedimiento de inicio de sesión y/o transacción en el dispositivo electrónico, también se puede pedir al usuario que introduzca un código que ha sido generado por el servidor, del cual se obtiene la primera clave (a su vez, por ejemplo, a petición del servidor del proveedor de servicios) y enviado al dispositivo electrónico como información de autenticación, por ejemplo, en una aplicación (por ejemplo, una página de Internet), a través de la cual el usuario ha realizado el procedimiento de inicio de sesión y/o transacción y que se ejecuta en el dispositivo electrónico o en otro dispositivo, por ejemplo, un dispositivo informático. Entonces se suministra el código, por ejemplo, al servidor del proveedor de servicios y de éste al servidor que ha generado el código para su verificación, y se devuelve el correspondiente resultado al servidor del proveedor de servicios.

Según una forma de realización de ejemplo de la invención, la comunicación se produce entre el dispositivo electrónico y el servidor y sirve para suministrar información de autenticación, que es necesaria para un procedimiento de inicio de sesión y/o transacción, que el usuario del dispositivo electrónico desea realizar con el dispositivo electrónico en un servidor de un proveedor de servicios, desde el servidor al dispositivo electrónico. La información de autenticación (por ejemplo, un código de una sola vez) puede, por ejemplo, ser recibido por el dispositivo electrónico y procesado o suministrado (por ejemplo, automáticamente) a una aplicación que se está ejecutando en el dispositivo electrónico a través de la cual el usuario realiza el procedimiento de inicio de sesión o de transacción, de modo que ya no sea necesario que el usuario introduzca manualmente la información de autenticación (tal como, por ejemplo, un nombre de usuario y/o una contraseña) en la aplicación. El usuario simplemente tiene que realizar una auto autenticación en relación con el servidor, del cual se obtiene la primera clave, y no es necesaria una nueva autenticación en relación con la aplicación. En este caso, por ejemplo, la aplicación puede ser parte de un software (por ejemplo, el software según la invención), que también realiza o controla el procedimiento según la invención, en la medida en que éste se realiza en el dispositivo electrónico, y/o la comunicación del dispositivo electrónico con el servidor. La aplicación puede ser, por ejemplo, una aplicación de navegador, por ejemplo, una aplicación de navegador seguro. Alternativamente, la aplicación también puede estar disponible por separado del software del dispositivo electrónico (por ejemplo, como un navegador) y al menos parcialmente utilizada y/o controlada por el software. A modo de ejemplo, el software puede integrar una aplicación de navegación independiente presente en el dispositivo electrónico en el software y hacer uso de sus funcionalidades (por ejemplo, como componente de visualización web).

Según una forma de realización de ejemplo de la invención, el procedimiento según la invención, realizado en el dispositivo electrónico, es realizado y/o controlado por software almacenado en el dispositivo electrónico. El software puede, por ejemplo, ser descargado como una aplicación (App) en el dispositivo electrónico e instalado en el mismo. El software se puede almacenar, por ejemplo, de forma no cifrada en el dispositivo. El software puede, por ejemplo, incluir un almacén de certificados con certificados de confianza (por ejemplo, de autoridades de certificación calificadas como fiables) y almacenarlos, por ejemplo, en el dispositivo electrónico. Las claves públicas de los certificados de este almacén de certificados se utilizan, por ejemplo, para comprobar los certificados recibidos o son utilizadas por ellos mismos sin necesidad de realizar más comprobaciones en la comunicación del software (ya que se consideran de confianza). Este almacén de certificados es, por ejemplo, un almacén de certificados diferente del almacén de certificados que estaba disponible antes de la instalación del software en el dispositivo electrónico. El almacén de certificados puede, por ejemplo, ser accesible exclusivamente sólo a través del software y/o modificable exclusivamente sólo a través del software. El software puede cifrar adicionalmente la segunda clave con la primera clave y almacenarla en el dispositivo. El software puede comprender o al menos controlar una aplicación (por ejemplo, una aplicación de navegador) para realizar procedimientos de inicio de sesión y/o transacción en un servidor de un proveedor de servicios (que, por ejemplo, difiere o se corresponde con el servidor del cual se obtiene la primera clave). El software puede, por ejemplo, controlar la aplicación de tal manera que sólo sean posibles procedimientos de inicio de sesión y/o transacción con, por ejemplo, servidores definidos por una lista blanca de URL. La aplicación de navegador puede, por ejemplo, ser un navegador seguro. El software puede incluir una pantalla para la aplicación de navegador y otra pantalla para los mensajes recibidos procedentes del servidor del cual se obtiene la primera clave.

Según una forma de realización de ejemplo de la invención, el procedimiento es realizado y/o controlado por un software o programa informático almacenado en el dispositivo electrónico, en el que se comprueba al menos una característica del programa informático y/o al menos una característica del dispositivo electrónico en la autenticación en relación con el servidor (por ejemplo, por parte del servidor) y sólo se obtiene la primera clave si la comprobación ha sido satisfactoria. La al menos una característica del software puede ser, por ejemplo, la integridad y/o la versión (en particular, la versión correcta, es decir, la versión más alta disponible actualmente) y/o la identidad y/o la asignación correcta del software al dispositivo electrónico. La al menos una característica del dispositivo electrónico

puede ser, por ejemplo, la integridad de los derechos de acceso de usuario previstos por el fabricante del dispositivo electrónico para el dispositivo electrónico (de este modo, se pueden excluir, por ejemplo, las manipulaciones por medio de las denominadas fugas de la cárcel o jailbreaks). También se pueden comprobar varias o todas estas características y, por lo tanto, la primera clave sólo se obtiene si todas las comprobaciones (y, además, la autenticación del usuario y/o del dispositivo, por ejemplo, mediante un PIN) se han realizado satisfactoriamente. Por ejemplo, el software se puede considerar intacto (o de total integridad) si se encuentra en el estado original o en un estado que se deriva del estado original sólo a través de actualizaciones oficiales. Esto se puede verificar, por ejemplo, mediante valores hash de imágenes del software (por ejemplo, en la memoria flash o la memoria RAM).

Según una forma de realización de ejemplo de la invención, el software almacenado en el dispositivo electrónico es un software de arranque o iniciador (por ejemplo, no cifrado). El software de arranque se ejecuta, por ejemplo, para obtener del servidor la primera clave. Con la primera clave, se pueden descifrar y utilizar los datos cifrados en el dispositivo electrónico (por ejemplo, una aplicación de comunicaciones o una parte de la misma, o la segunda clave). El software de arranque también puede ser configurado para que ejecute una fase de inicialización en la que un usuario del dispositivo electrónico (y/o el dispositivo electrónico) realiza la auto autenticación en relación con el servidor y, en caso de autenticación satisfactoria, recibe la primera clave para cifrado de datos para la recepción de los datos cifrados. Si los datos descifrados comprenden software para la comunicación del dispositivo electrónico, este software junto con el software de arranque (y posiblemente otros componentes) pueden formar un paquete de software (por ejemplo, no cifrado) que, por ejemplo, puede ser cargado en el dispositivo electrónico como una aplicación. Alternativamente, se pueden utilizar varios paquetes de software/aplicaciones.

De acuerdo con una forma de realización de ejemplo de la invención, los datos descifrados comprenden software para la comunicación del dispositivo electrónico. El software puede ser, por ejemplo, una aplicación que se puede descargar de un servidor para aplicaciones, por ejemplo, una aplicación de banca en línea, o para el control remoto de componentes o el acceso remoto a datos o programas. El software puede ser, por ejemplo, un navegador. A modo de ejemplo, el software se almacena al menos parcialmente cifrado en el dispositivo electrónico. En particular, el software es al menos una parte de los datos almacenados con cifrado en el dispositivo electrónico, que se pueden descifrar con la primera clave. Esto es, entre otras cosas, ventajoso con el fin de individualizar el software para cada usuario (y/o cada dispositivo electrónico) (al menos si la primera clave es individual para el usuario), lo que dificulta la ingeniería inversa del software. Además, esto es, entre otras cosas, ventajoso puesto que un atacante, incluso si está en posesión del dispositivo electrónico, debe realizar satisfactoriamente la auto autenticación en relación con el servidor, con el fin de poder utilizar la comunicación del dispositivo electrónico.

De acuerdo con una forma de realización de ejemplo de la invención, el software que realiza y/o controla el procedimiento es seguro.

Según una forma de realización de ejemplo de la invención, el software para la comunicación del dispositivo electrónico es seguro.

En términos de medios seguros de ingeniería de programación que, por ejemplo, sólo utilizan dicho software (dedicado) necesario para el funcionamiento del sistema y cuyo funcionamiento seguro se puede garantizar en términos de seguridad. De este modo, en el caso del software seguro (por ejemplo, un navegador) se pueden eliminar todos los componentes y funciones del software que no sean absolutamente necesarios para realizar la tarea prevista por el software. Una función de securización también puede incluir mecanismos de anti ingeniería inversa, anti depuración y/o anti inyección de código.

Según una forma de realización de ejemplo de la invención, el software es una aplicación adaptada para el dispositivo electrónico. Una aplicación es, en particular, una denominada App, que puede ser obtenida por el dispositivo electrónico de una denominada "App Store", por ejemplo, en el caso de un teléfono móvil o de un dispositivo informático (tableta).

Según una forma de realización de ejemplo de la invención, el procedimiento, realizado en el servidor, en una fase de inicialización también comprende suministrar la primera clave al dispositivo electrónico para el cifrado de los datos en el dispositivo electrónico, en el que el suministro sólo se produce tras la autenticación satisfactoria del usuario (y/o del dispositivo electrónico) por parte del servidor.

Según una forma de realización de ejemplo de la invención, el procedimiento, realizado en un servidor, también comprende en una fase de inicialización la generación (por ejemplo aleatoria) de la primera clave.

Las formas de realización de ejemplo y las configuraciones de ejemplo descritas en esta especificación de la presente invención también se consideran divulgadas en todas las combinaciones entre las mismas. Se pueden inferir configuraciones adicionales de ejemplo ventajosas a partir de la siguiente descripción detallada de formas de realización de ejemplo de la presente invención, en particular junto con las Figuras.

Sin embargo, las Figuras que acompañan a la solicitud deben servir únicamente para aclarar y no para determinar el alcance de protección de la invención. Los dibujos adjuntos no son a escala y sólo reflejan el concepto general de la presente invención. En particular, las características que se muestran en las Figuras no se deben considerar de ninguna manera como un componente necesario de la presente invención.

Breve descripción de los dibujos
Las Figuras son las siguientes

Figura 1: una representación esquemática de los componentes de una forma de realización de ejemplo de un sistema según la invención y un ejemplo de secuencia de las interacciones entre los componentes;

Figura 2: un ejemplo de una secuencia de un procedimiento según la invención;

Figura 3 – 5b: ejemplos de escenarios de aplicación de la invención;

Figura 6 – 8: ejemplos de escenarios para el almacenamiento de una clave secreta según la invención;

Figura 9: una representación esquemática de los componentes de una forma de realización de ejemplo de un dispositivo electrónico según la invención;

Figura 10: una representación esquemática de los componentes de una forma de realización de ejemplo de un servidor según la invención; y

Figura 11: una representación esquemática de una forma de realización de ejemplo de un medio de almacenamiento según la invención.

Descripción detallada de algunas formas de realización de ejemplo de la presente invención
Configuraciones de ejemplo de la invención contienen un esquema de autenticación y cifrado que puede ser implementado en un dispositivo electrónico, por ejemplo en forma de software (por lo tanto, un programa informático). Este esquema incluye un enlace estrecho (close link) con un servidor, que en adelante será denominado servidor SSMS (smart Security Management Server – Servidor de Administración de Seguridad Inteligente) y que funciona como un anclaje de seguridad adicional. Este enlace hace una contribución considerable a la mayor seguridad conseguida con la invención. El servidor SSMS sirve, por ejemplo, para administrar los dispositivos y el software. Esto puede ser proporcionado por un proveedor de servicios independiente del banco o por el propio banco para permitir la banca en línea.

En lo sucesivo, se asume a menudo que el dispositivo electrónico es un teléfono inteligente (smartphone) y el software una aplicación (o "App"), pero la presente invención no se limita a dichas configuraciones.

La seguridad puede aumentarse utilizando opcionalmente un componente de hardware adicional, que por ejemplo puede conectarse por medio de un enlace inalámbrico, por ejemplo un enlace Bluetooth, al dispositivo electrónico.

Formas de realización de ejemplo de la invención proporcionan una solución segura para dispositivos electrónicos (en lo sucesivo denominados a modo de ejemplo terminales móviles) tales como, por ejemplo, teléfonos inteligentes. Hay un control individual de cada instancia de software. El servidor SSMS se utiliza como una instancia de autenticación segura (en la que la autenticación significa tanto el proceso en el que un usuario demuestra su propia identidad (por ejemplo, en relación con un servidor) como el proceso de comprobar la evidencia de la identidad de un usuario (por ejemplo, por parte de un servidor)).

Ejemplos típicos de la invención son, por ejemplo:
- un software o programa informático, en particular un programa informático de banca en línea (por ejemplo, un navegador), que está presente en el dispositivo electrónico o puede ser cargado en el mismo, o
- un kit de desarrollo de software (SDK – software development kit), con el que se puede crear el software o una aplicación para dispositivos electrónicos.

Según ya se ha mencionado, opcionalmente también se puede añadir un componente de hardware.

Ejemplos de plataformas para este tipo de software son iOS o Android de Apple. Por supuesto, la aplicación también puede ser posible en dispositivos electrónicos con sistema operativo Windows, Linux o BlackBerry.

En formas de realización de la invención, el programa informático según la invención funciona en plataformas móviles (por ejemplo, terminales móviles, por ejemplo, teléfonos móviles, PDA, dispositivos informáticos portátiles o

dispositivos informáticos de tableta) y proporciona una serie de funciones de seguridad integradas, que comprenden una o más de las siguientes características:
- Protección contra la depuración (debugging) e ingeniería inversa;
- Procedimientos adicionales de securización (hardening) de software para la protección contra ataques conocidos en tiempo de ejecución;
- Protección de URL para servicios en línea (tales como por ejemplo direcciones URL de bancos);
- Un almacén de certificados integrado para certificados de autoridades de certificación de confianza (CA - Certificate Authorities) y/o para certificados personales. Este almacén de certificados está, por ejemplo, enlazado con el software según la invención y, en particular, no corresponde al almacén de certificados presente en el terminal móvil (como, por ejemplo, ya presente en el momento de la instalación del software). De esta forma se obtiene una seguridad más precisa, ya que sólo se deben almacenar los certificados que son exactamente relevantes para la aplicación respectiva (por ejemplo, para la configuración/prueba de enlaces SSL con los servidores de proveedores de servicios y/o con el servidor SSMS). El software puede, por ejemplo, utilizar exclusivamente sólo aquellos certificados que se encuentran en el almacén de certificados conectado al mismo (por ejemplo, los que originalmente estaban contenidos en el mismo y/o los importados por el software al almacén de certificados). Los datos en el almacén de certificados pueden ser no cifrados o cifrados, por ejemplo, con la clave secreta del terminal móvil, que sólo está disponible tras la autenticación en el servidor SSMS. El acceso al almacén de certificados sólo es posible, por ejemplo, tras una autenticación satisfactoria en el servidor SSMS.

Estas funciones de seguridad evitan los ataques fuera de línea, cuyo objetivo es encontrar puntos débiles e investigar información privada de los usuarios. La protección de URL asegura que los usuarios alcanzan el servicio en línea correcto. El almacén de certificados integrado protege contra certificados digitales y anclajes de confianza (autoridades de certificación) no legítimos en el almacén de certificados estándar del terminal móvil. Estos certificados falsos pueden, por ejemplo, ser importados tácitamente o las autoridades de certificación que antes se consideraban fiables pueden, por ejemplo, haber sido revocadas mientras tanto, pero sin que el terminal móvil se haya actualizado todavía a este respecto.

El software según la invención está acoplado con un servidor dedicado (el servidor SSMS), está protegido por el mismo y es administrado por el mismo. El servidor SSMS es alojado por un proveedor de servicios en línea (por ejemplo, un banco) y está integrado, por ejemplo, en los servicios en línea (tal como un navegador web de un banco). El servidor SSMS genera junto con el software según la invención, que por ejemplo funciona como una aplicación en el terminal móvil, una instancia de un dispositivo virtual en el terminal móvil, que convierte el terminal móvil en un aparato de autenticación único. Cuando el software se está activando por primera vez, el software es enlazado o vinculado con el dispositivo móvil dedicado en el que está instalado y es registrado en el servidor SSMS. Siempre que el software es llamado, el servidor SSMS realiza una serie de comprobaciones con el software, por ejemplo, una o más de las siguientes comprobaciones:
- si el software se está ejecutando realmente en el terminal móvil dedicado o ha sido copiado en otro dispositivo (esto se puede comprobar, por ejemplo, utilizando un número de identificación del terminal móvil, tal como, por ejemplo, un identificador IMEI (International Mobile Equipment Identity – Identidad de equipo móvil internacional) o MAC (Medium Access Control – Control de acceso al medio), u otra característica y única característica del terminal móvil, por ejemplo, una huella electromagnética del terminal móvil realizando, por ejemplo, una comprobación de si los valores relevantes se desvían de los valores presentes en el momento del registro del software en el servidor SSMS);
- si el software se encuentra todavía en su estado original o si ha sido modificado (esto se puede determinar, por ejemplo, utilizando un valor hash del software, por ejemplo, en la memoria RAM o memoria flash);
- si la versión del software es correcta o se debe actualizar;
- si el PIN de usuario (o una contraseña) introducido es correcto;
- si el terminal móvil dedicado ha sido provisto con derechos de acceso de usuario (por ejemplo, "derechos de raíz") superiores a los previstos por el fabricante, por ejemplo, con el fin de poder instalar otras aplicaciones (por ejemplo, aplicaciones manipuladoras) en el terminal móvil. Esta comprobación constituye la denominada "detección de fuga de la cárcel o jailbreak".

Estas comprobaciones permiten impedir ataques basados en programas informáticos falsificados para el acceso a servicios en línea o en programas informáticos modificados para modificar datos de acceso o de transacción (por ejemplo, aplicaciones falsificadas o modificadas). Los atacantes tendrían el control tanto del terminal móvil como del servidor SSMS simultáneamente, con el fin de romper la cadena de confianza. Sin embargo, ambos extremos se controlan entre sí y, como resultado, pueden poner fin a cualquier actividad sospechosa. El PIN (o contraseña) del usuario nunca se almacena ni se almacena en caché en el terminal móvil, sino que más bien se trata de un PIN de autenticación del servidor. Si, por ejemplo, se introduce un PIN incorrecto tres veces, el PIN del usuario es bloqueado en el servidor SSMS.

El software según la invención proporciona junto con el servidor SSMS un canal de comunicación independiente y seguro. Si el software es instalado en un terminal móvil, con el que se accede a los servicios en línea de un servidor

(por ejemplo, de un servidor bancario), el enlace entre el software y el servidor SSMS (el canal de comunicación independiente y seguro antes mencionado) se considera independiente con respecto al enlace utilizado para este acceso. Si para el acceso a los servicios en línea de un servidor (por ejemplo, de un servidor bancario) se utiliza un dispositivo informático, el enlace entre un terminal móvil, en el que está instalado el software, es igualmente independiente del enlace utilizado para este acceso entre el dispositivo informático y el servidor. En general, por lo tanto, se establece una técnica de comunicación dual. El software según la invención puede, por ejemplo, formar parte de un software de banca en línea (por ejemplo, una aplicación), que funciona en un terminal móvil. El servidor SSMS se comunica con los servicios en línea o los servidores que los proporcionan (o es parte de este servidor). El canal de comunicación entre el software y el servidor SSMS es, por lo tanto, diferente de los canales de comunicación convencionales utilizados para acceder a servicios en línea (que en el estado actual de la técnica se consideran "seguros"). Es particularmente ventajoso que los ataques genéricos en estos canales de comunicación convencionales no tienen ningún efecto en la seguridad del canal de comunicación entre el software y el servidor SSMS (ya que, por ejemplo, el almacén protegido de certificados del software no se ve afectado por dichos ataques).

Formas de realización del software según la invención proporcionan, junto con el servidor SSMS, una o más de las siguientes funciones:
- El software tiene un enlace seguro integrado con el servidor SSMS dedicado (por ejemplo, el servidor SSMS en el que está registrado).
- El servidor SSMS tiene toda la información sobre el software registrado y realiza las funciones de control descritas anteriormente.
- El servidor SSMS puede personalizar el software de forma remota (por ejemplo, con información específica de usuario).
- El servidor SSMS codifica y protege los datos privados del software.
- En esta segunda vía de comunicación (entre el software y el servidor SSMS) hay un cifrado y una autenticación de extremo a extremo.

Estas funciones evitan ataques de intermediario (man-in-the-middle attacks) y garantizan la confidencialidad e integridad de los datos. Los proveedores de servicios en línea (por ejemplo, un banco) pueden, por ejemplo, requerir confirmaciones de inicio de sesión y/o de transacciones procedentes del servidor SSMS. La confirmación y la verificación del usuario ya están integradas en este segundo canal de comunicación.

Formas de realización de la presente invención tienen las siguientes ventajas sobre los procedimientos de autenticación que se listan a continuación:
- Se puede evitar el envío de SMS (Short Message Services) con contraseñas de un solo uso (OTP) como procedimiento de autenticación alternativo, en el que el envío de cada SMS (incluso con un paquete) puede tener un coste de entre 6 y 10 céntimos de euro y pueden ser espiados con relativa facilidad por software malicioso y/o desautorizados por la redirección o el reenvío de SMS.
- Se puede evitar el uso de software/aplicaciones para la generación de contraseñas de un solo uso (OTP) en terminales móviles como un procedimiento alternativo de autenticación. Este software de contraseñas OTP puede, por ejemplo, ser copiado a otros terminales móviles u dispositivos informáticos y es susceptible a ataques fuera de línea, por ejemplo, mediante depuración, ingeniería inversa y ataques de fuerza bruta para descubrir el PIN de la aplicación, que por lo general sólo consta de 4 o 6 dígitos (incluso aunque el software de contraseñas OTP se bloquee después de 3 intentos incorrectos del PIN, se dispone de un número infinito de otras copias del software de contraseñas OTP para más intentos). Las contraseñas OTP utilizadas generalmente no están relacionadas con las transacciones y, por lo tanto, no son susceptibles a la suplantación de identidad (phishing), al pharming, a ataques de intermediario y a ataques de intermediario en navegador. Si las contraseñas OTP son específicas de transacción, el usuario normalmente debe introducir los datos de transacción dos veces, una en el dispositivo informático, en el que se produce el acceso al proveedor de servicios, y otra en el terminal móvil, en el que se genera luego la contraseña OTP. Esto es susceptible a fallos y no es muy fácil de utilizar.
- También se puede evitar el uso de tokens de hardware dedicados (por ejemplo, generadores de números de transacción, TAN). La necesidad de dicho dispositivo adicional se percibe al menos como una molestia en comparación con, por ejemplo, el uso de un teléfono móvil que también tiene otros usos. Básicamente, estos tokens de hardware están sujetos a los mismos problemas que el software de contraseñas OTP. Además, las soluciones de contraseñas OTP se basan a menudo en un cifrado simétrico, de modo que la clave debe estar presente en al menos el servidor de verificación y, en teoría, puede ser utilizada en el mismo.
- Se evita el suministro de certificados de software para terminales móviles por parte del proveedor de servicios en línea, cuya aplicación es costosa y complicada (en particular, por lo que se refiere a la emisión y verificación). De nuevo, con los certificados de software existe el peligro, al igual que con el software de contraseñas OTP, de que los atacantes accedan al almacén de certificados de todo el sistema de los terminales móviles (estando, de este modo, el almacén de certificados ya presente en el momento de la entrega del dispositivo) y/o copien las claves secretas.

Formas de realización de ejemplo de la presente invención no utilizan ni servicios SMS ni software de contraseñas OTP. En su lugar, se utilizan certificados digitales seguros como certificados de usuario, que sin embargo no tienen que ser emitidos y verificados por el proveedor de servicios (por ejemplo, un banco), ya que esta tarea es asumida por el servidor SSMS. Así se obtiene una o más de las siguientes ventajas:

- Los certificados de usuario se basan en claves criptográficas asimétricas (secretas y públicas). Sólo el usuario está en posesión de la clave secreta única (en forma cifrada), y no hay copia de la clave secreta en el servidor SSMS (ni en ningún otro servidor).
- El servidor SSMS tiene una autoridad de certificación (CA) integrada para suministrar certificados de usuario. Los principales componentes de software de esta autoridad de certificación proceden, por ejemplo, de una solución de centro de confianza evaluado por Criterios Comunes (CC) EAL 3+. No hay costes adicionales por cada certificado de usuario.
- El servidor SSMS puede suministrar certificados de usuario para cada software registrado de acuerdo con la invención, en el que no se recopila información de usuario y tampoco se tiene que implementar y administrar ningún proceso complicado de despliegue. El despliegue de los certificados se realiza sin problemas para el usuario y el proveedor de servicios en línea. Los certificados contienen la respectiva clave pública del par asimétrico de claves, que se genera en el respectivo software según la invención, son firmados en el servidor SSMS en base a la autoridad de certificación, y luego son suministrados, por ejemplo, al respectivo software según la invención o a otras entidades.
- Ambos componentes (servidor SSMS y software según la invención) pueden enviar mensajes (auténticos) firmados al otro y verificar las firmas digitales consecuentemente.
- El software según la invención contiene un almacén de certificados integrado para certificados procedentes de autoridades de certificación de confianza (CA) y/o para certificados personales.
- Los datos locales del software según la invención pueden ser cifrados con una clave única, administrada en el servidor SSMS asignado (por ejemplo, en el terminal móvil). Los datos locales cifrados pueden comprender, por ejemplo, una clave secreta del terminal móvil, que está destinada a la comunicación del dispositivo móvil (por ejemplo, para una autenticación en el contexto de esta comunicación). Opcionalmente, el almacén de certificados también puede ser cifrado.

En formas de realización de la invención, los proveedores de servicios en línea pueden hacer uso de las ventajas de la invención, utilizando programas informáticos de acuerdo con la invención (por ejemplo, como parte de programas informáticos de aplicación más amplios que sirven para acceder al servidor de aplicaciones del proveedor de servicios en línea, por ejemplo, una aplicación de banca en línea) en terminales móviles y con el servidor de aplicaciones que se comunica con el servidor SSMS, si es necesario confirmar un procedimiento de inicio de sesión y/o transacción. El servidor de aplicaciones y el software de aplicación se comunican en una capa lógica relacionada con el proceso de negocio, mientras que el software de acuerdo con la invención y el servidor SSMS introducen una capa relacionada con la seguridad dual con la capa relacionada con el proceso de negocio y se comunican en la misma.

El software según la invención se puede proporcionar, por ejemplo, en el contexto de un kit de desarrollo de software (SDK) y luego ser utilizado por los desarrolladores para adaptar el software de aplicación existente o para crear un nuevo software de aplicación.

La interfaz en el lado del cliente comprende, por ejemplo, sólo unas pocas llamadas de función básicas, que simplemente tienen que ser integradas en el software de aplicación. El kit SDK puede, por ejemplo, incluir una biblioteca binaria y un código fuente para la demostración de las diferentes llamadas de función. La comunicación se realiza a través de una interfaz asíncrona, que no bloquea el software de aplicación mientras se realizan las funciones de seguridad.

La interfaz en el lado del servidor se puede crear, por ejemplo, utilizando el protocolo simple de acceso a objetos (SOAP: Simple Object Access Protocol), que es independiente de los lenguajes de programación. El servidor SSMS es, por ejemplo, un servidor independiente, que debería funcionar en un entorno seguro. Cuando el servidor SSMS requiere una confirmación de un inicio de sesión o de un procedimiento de transacción, esto se puede realizar, por ejemplo, a través de una consulta del protocolo SOAP desde el servidor de aplicaciones al servidor SSMS. El servidor SSMS también puede generar un código de activación para el registro de usuario, que puede ser solicitado por el servidor SSMS mediante consultas del protocolo SOAP desde el servidor de aplicaciones.

En formas de realización de ejemplo de la invención, el servidor SSMS proporciona códigos de activación únicos para cada plataforma móvil. Si un usuario accede a los servicios en línea con varios dispositivos, recibirá, por ejemplo, unos códigos de activación para cada uno de estos dispositivos por derecho propio. Los códigos de activación pueden ser distribuidos por el proveedor de servicios, en función de sus directrices internas de seguridad, por ejemplo, a los usuarios finales por medios impresos (cartas, etc.), por SMS a números de teléfono móvil pre-registrados, a través de centros de llamadas (una vez que el usuario llamado ha respondido correctamente a las preguntas de seguridad predefinidas), a través de sucursales (cara a cara) o a través de un sitio de Internet, en el

que el usuario ha realizado satisfactoriamente la auto autenticación (por ejemplo, con su autenticación utilizada anteriormente, por ejemplo, con una contraseña estática, de protocolo OTP, de servicio SMS, de protocolo OTP de voz en pantalla, etc.).

En formas de realización de la invención -por ejemplo, utilizando el kit SDK- se genera un software de aplicación genérico como una "aplicación" o "App" con el software según la invención integrado y preconfigurado en la misma, y es cargado en uno o más "Almacenes de Aplicaciones". El software según la invención (como parte del software de aplicación) está por ejemplo preconfigurado para una determinada dirección URL de servidor SSMS. Como el certificado de servidor de confianza, en el software según la invención (por ejemplo, en su almacén de certificados), por ejemplo el certificado del servidor, que está alojado y administrado por el proveedor de servicios en línea (por ejemplo, un banco), puede ser preconfigurado. El usuario descarga el software de aplicación con el software según la invención del "Almacén de Aplicaciones". Con el fin de aumentar la seguridad, se puede proporcionar que el usuario, junto con el código de activación, sea informado del enlace legítimo en el que puede descargar el software de aplicación. Si se descarga el software de aplicación incorrecto, el servidor SSMS lo puede detectar y detener la comunicación con el usuario.

Según se describe más detalladamente a continuación, con el fin de utilizar el software de aplicación con el software integrado según la invención por primera vez, se requiere la introducción del código de activación y la definición de un PIN (o una contraseña) por parte del usuario. Todos los demás procesos de registro, entrada y personalización se ejecutan automáticamente y sin problemas desde el punto de vista del usuario. El PIN se almacena en el servidor SSMS y se verifica en el mismo cada vez que el usuario reinicia el software de aplicación, con el fin de realizar la auto autenticación. Sin embargo, no se almacena en el terminal móvil del usuario, ni siquiera de forma cifrada. Múltiples entradas incorrectas del PIN provocan el bloqueo de la cuenta de usuario en el servidor SSMS, de modo que en caso de robo del terminal móvil no es posible utilizar la función de autenticación del terminal móvil ni la extracción del PIN. Si el PIN se pierde después de una nueva ejecución de la comprobación de seguridad, por ejemplo, se puede enviar un código de activación al usuario (en los canales mencionados anteriormente).

Tras la introducción de un PIN válido, todos los procesos de registro en el servidor SSMS y la comprobación de seguridad del software de aplicación son realizados automáticamente por el servidor SSMS. Si, por ejemplo, el usuario debe confirmar los procedimientos de inicio de sesión o de transacción, se muestra un correspondiente texto auténtico para su confirmación o rechazo en el terminal móvil. En caso de confirmación, es firmado por el software de acuerdo con la invención utilizando una clave secreta y enviado al servidor SSMS, que verifica el mensaje firmado e informa al servidor de aplicación de la confirmación. Los procesos de firma y verificación se ejecutan sin problemas desde el punto de vista del servidor de aplicaciones. En el caso de transacciones con riesgo, si es necesario, el usuario puede solicitar la reintroducción del PIN.

En formas de realización de la invención se aplica el siguiente concepto:
- se descarga el software (por ejemplo, en forma de aplicación) de un servidor, por ejemplo, un "Almacén de Aplicaciones" (App Store), al dispositivo electrónico;
- el servidor SSMS se utiliza como anclaje de seguridad para el software;
- se cifran datos locales relativos al dispositivo electrónico del software con una clave (por ejemplo, una clave según el estándar AES), que el servidor SSMS recibe durante la sesión (los datos locales pueden, por ejemplo, formar parte del software, por ejemplo, una parte que implementa al menos parcialmente una funcionalidad de banca en línea; alternativa o adicionalmente, los datos locales pueden incluir una clave secreta para la autenticación, la firma y/o el cifrado);
- cada vez que se utiliza o se inicia el software se produce una autenticación en relación con el servidor SSMS;
- el software puede ser, al menos parcialmente, securizado, entre otras cosas contra la ingeniería inversa.

La Figura 1 es una representación esquemática de los componentes de una forma de realización de ejemplo de un sistema 1 según la invención y una secuencia de ejemplo de las interacciones entre los componentes. En este caso, se distingue entre una fase inicial de activación del software/aplicación (que se muestra a la izquierda) y una fase en la que se utiliza el software/aplicación (a la derecha).

El software se descarga, por ejemplo, de un almacén o tienda de aplicaciones 4 al dispositivo electrónico 3 y, por ejemplo, se inicializa al menos parcialmente en el mismo. Una parte del software (por ejemplo, el software de arranque o iniciador) sirve para ejecutar y/o controlar las etapas (2) y (3). Esta parte del software (u otra parte) también puede ejecutar y/o controlar las etapas (1') y (2'). Otra parte del software puede entonces, por ejemplo, ejecutar y/o controlar la etapa (3').

El software establece primero un enlace seguro (por ejemplo, un enlace SSL) entre el dispositivo electrónico 2 y el servidor SSMS 3. La autenticación en el lado del servidor (del servidor SSMS 3) se basa en este caso, por ejemplo, en un certificado precodificado (que, por ejemplo, se almacena en el dispositivo electrónico 2 (por ejemplo, este certificado ha sido instalado con o por el software del dispositivo electrónico) y se puede utilizar para comprobar un

certificado del servidor SSMS), y la autenticación en el lado del cliente (del dispositivo electrónico 2) se basa, por ejemplo, en una clave de activación (que, por ejemplo, puede ser recibida por correo postal o por correo electrónico) o en un número de identificación personal (PIN), que, por ejemplo, se puede haber configurado durante la activación. El PIN y la activación tienen básicamente una función similar en este caso, pero en diferentes momentos: durante el inicio de sesión el usuario realiza una auto autenticación con el código de activación. Esto es válido sólo una vez y luego expira. En la misma etapa el usuario también debe definir un PIN (que es suministrado al servidor SSMS junto con el código de activación), que a partir de ahora debe ser utilizado para todos los accesos futuros.

El software almacena al menos parte de los datos (por ejemplo, software para la comunicación con el banco 5, o datos que utilizan este software para la comunicación con el banco 5, tal como por ejemplo, una clave secreta o un certificado) de forma cifrada (por ejemplo, en base a un cifrado simétrico o asimétrico), por ejemplo, por medio de un cifrado AES. La clave proviene del servidor SSMS 2 (etapa (3)) y nunca se almacena localmente en el dispositivo 3. El software sólo puede descifrar los datos si ha iniciado sesión en el servidor SSMS 2.

Durante la fase de activación se genera un certificado de cliente en el software y firmado por el servidor SSMS 2 (etapa (3)). Este certificado se utiliza, por ejemplo, para realizar operaciones bancarias en línea con un banco 5. La clave secreta asociada nunca sale del software (y del dispositivo 3). Por ejemplo, está cifrado con la clave según el estándar AES en el dispositivo 3 y almacenado en el mismo.

Cada vez que se utiliza o se inicia el software, se realiza un inicio de sesión en el servidor SSMS 2 (etapa (1')), para recibir la clave (etapa (2')). El servidor SSMS 2 puede, por ejemplo, realizar una comprobación de la versión del software en el dispositivo 3 y actualizar o bloquear el software obsoleto. También es posible que el servidor SSMS 2 realice otras comprobaciones, por ejemplo, sobre la integridad del software, la versión del software, si el software está instalado en el dispositivo electrónico (correcto) 3 y/o si los derechos de acceso de usuario proporcionados por el fabricante para el dispositivo electrónico (por ejemplo, en lo que se refiere a la autorización del usuario, para instalar y/o cambiar programas en el dispositivo electrónico) han permanecido inalterados (detección de una "fuga de la cárcel" o “jailbreak”). Debido a la necesidad de realizar un inicio de sesión hay un control completo por parte del usuario.

En la Figura 2 se muestra una secuencia de un procedimiento de ejemplo según la invención, en el que inicialmente se supone una fase de personalización para el software. En esta fase se instala el software y es iniciado por primera vez (por ejemplo, por medio de un software de arranque no cifrado). En este caso, para empezar, se establece un enlace SSL/TLS con (por ejemplo, simplemente) autenticación en el lado del servidor. Para ello, el servidor SSMS envía al software un certificado que el software puede comprobar con la clave pública (KOBIL) que está presente en el mismo (alternativamente, también puede estar presente un certificado del servidor SSMS en el software (por ejemplo, en el almacén de certificados para certificados de confianza), de modo que se puede prescindir de una comprobación).

Con la clave pública del certificado, el software cifra una clave de sesión, en la que se basa el cifrado de los datos del enlace SSL, y envía la clave de sesión cifrada al servidor SSMS. El servidor SSMS descifra la clave de sesión con la clave secreta asociada que se encuentra presente en el mismo. Esto completa la autenticación del servidor. La clave pública (KOBIL), que se almacena en el software, funciona en este caso como un anclaje de confianza. Por lo tanto, el software debe reconocer esencialmente sólo la clave pública KOBIL o el certificado asociado y no el certificado de cada instancia de servidor SSMS, al que el software puede estar vinculado o enlazado. A modo de ejemplo, si el certificado del servidor SSMS enviado por el software (que por ejemplo contiene la clave pública del servidor SSMS) es firmado con la clave secreta (KOBIL) de la autoridad de certificación raíz de KOBIL, entonces el software puede comprobar la validez de este certificado con la clave pública KOBIL. Entonces el software puede ser utilizado de forma ventajosa con varios servidores SSMS, siempre y cuando éstos utilicen certificados de servidor SSMS, los cuales son firmados con la clave secreta (KOBIL) de la autoridad de certificación raíz de KOBIL.

En el certificado del servidor SSMS que se envía al software, se puede generar, por ejemplo, en lugar de la clave pública del servidor SSMS, una clave pública, generada especialmente para el cifrado de la clave de sesión, de un par asimétrico de claves que el servidor SSMS puede firmar (por ejemplo, con la clave secreta (KOBIL), por ejemplo, con el fin de evitar que cada vez que se establece un enlace seguro se utilice la misma clave para el cifrado de la clave de sesión. Alternativamente, el servidor SSMS también puede generar un sub-certificado con una clave pública para su uso en el cifrado de la clave de sesión y firmarla con la clave secreta del servidor SSMS. Entonces se puede comprobar la validez de este sub-certificado utilizando el certificado del servidor SSMS en el software, que a su vez se puede comprobar utilizando la clave pública (KOBIL).

En el software se genera un par de claves que comprenden una clave "pública" y otra "secreta" (o "privada") (por ejemplo, un par de claves RSA (según Rivest, shamir, Adleman)). La clave pública es firmada por el servidor SSMS (por ejemplo, con la clave secreta (KOBIL) o con la clave secreta del servidor SSMS) y, por ejemplo, suministrada al servidor bancario descrito a continuación. Alternativamente, la clave pública permanece en el servidor SSMS. De

este modo, el servidor SSMS puede generar los certificados de usuario basados en la autoridad de certificación raíz de KOBIL (con la respectiva clave pública del software), que se pueden utilizar para la autenticación del software, por ejemplo del servidor bancario u otros servidores que confían en la autoridad de certificación raíz de KOBIL.

La clave secreta es cifrada con una clave en el dispositivo, en este caso, a modo de ejemplo, una clave según el estándar AES, generada por el servidor SSMS. Además, algunas partes del propio software pueden ser cifradas con la clave, de modo que estas partes sólo son ejecutables si se ha recibido la clave procedente del servidor SSMS. Esto asegura que incluso si el software es leído, se dificulte la ingeniería inversa, ya que está parcialmente cifrada y la clave también es individual (relacionada con el dispositivo y/o el usuario).

En la fase de "uso normal" previa al uso real del software (en este caso, por ejemplo, banca en línea con un servidor bancario), se establece un enlace con el servidor SSMS para recibir la clave según el estándar AES para descifrar la clave secreta cifrada (y cualquier parte del software cifrada) en el dispositivo (por ejemplo, por medio de un software de arranque no cifrado). Además, opcionalmente, en este caso se puede recibir más información, tal como un certificado procedente del servidor bancario y/o una lista blanca.

Entonces, se utiliza la clave secreta en la comunicación (por ejemplo, para cifrar/firmar mensajes) con el servidor bancario (que, por ejemplo, ha recibido previamente la clave pública firmada por el servidor SSMS, que pertenece a la clave secreta). En el presente caso, se establece un enlace SSL/TLS con autenticación en el lado del cliente y del servidor, por ejemplo, de acuerdo con el documento de solicitud de comentarios (RFC) 5246 "The Transport Layer security (TLS) Protocol Version 1.2". La autenticación del servidor bancario en relación con el software se basa en el certificado del servidor bancario, que ha sido enviado previamente (opcionalmente) por el servidor SSMS al software. Este certificado puede, por ejemplo, ser firmado por el servidor SSMS (o por otra entidad) (por ejemplo, con la clave secreta (KOBIL) y luego comprobado utilizando la clave pública (KOBIL) que está presente en el software (por ejemplo, en su almacén de certificados para certificados de confianza). Alternativamente, el certificado del servidor bancario también puede ser firmado por otra entidad, siempre que el software de su almacén de certificados de confianza tenga una correspondiente clave pública para comprobar la firma. Como alternativas adicionales, el certificado del servidor bancario con su clave pública también se puede almacenar en el almacén de certificados para certificados de confianza del software, por lo que no es necesario volver a comprobar el certificado. La autenticación del servidor bancario se puede realizar, por ejemplo, por medio del software que cifra una clave de sesión (o un número aleatorio, a partir del cual se deriva la clave de sesión) con la clave pública del servidor bancario (del certificado) y el servidor bancario sólo puede descifrar esta información cifrada con su clave secreta.

La autenticación del software se basa en un certificado, que contiene la clave pública generada en el software. Este certificado ha sido previamente firmado por el servidor SSMS y enviado al servidor bancario, según se ha descrito anteriormente. A modo de ejemplo, el software puede firmar información (por ejemplo, una petición u otra información específica de sesión recibida procedente del servidor bancario) con la clave secreta. La firma puede entonces ser comprobada por el servidor bancario utilizando la clave pública del certificado recibido procedente del servidor SSMS y, por lo tanto, el software puede ser autenticado.

Adicional o alternativamente, la clave secreta también se puede utilizar para la comunicación con el servidor SSMS, por ejemplo, para configurar un enlace seguro (por ejemplo, cifrado) (por ejemplo, un enlace cifrado, que al menos se basa en la autenticación en el lado del cliente (y preferiblemente también en el lado del servidor), por ejemplo, un enlace SSL o TLS con autenticación en el lado del cliente y en el lado del servidor), y/o para la firma de mensajes (con la clave secreta), que son enviados al servidor SSMS. Si los mensajes firmados por el dispositivo 3 son enviados al servidor SSMS, por ejemplo para la confirmación de un procedimiento de inicio de sesión o transacción, estos mensajes firmados se pueden archivar, por ejemplo, en el servidor SSMS o en el servidor bancario, con el fin de disponer de pruebas en un momento posterior de la confirmación del procedimiento de inicio de sesión o transacción. La clave secreta puede ser utilizada adicional o alternativamente para cifrar los mensajes enviados al servidor SSMS.

En este caso el software asegura que la clave secreta (y la clave según el estándar AES) después de haber sido utilizada exitosamente es borrada de nuevo (sin embargo, puede, por ejemplo, después de una solicitud repetida de la clave según el estándar AES, ser descifrada de nuevo y utilizada por el servidor SSMS). Por ejemplo, la clave secreta sólo se puede almacenar en la memoria RAM, y no en la memoria FLASH. La desactivación de esta función se puede evitar mediante una securización adecuada del software.

Desde el punto de vista del usuario, por lo tanto, existen dos escenarios de uso diferentes:

1. Activación
- Se realiza una vez por instalación del software en el dispositivo.
- La clave de activación es recibida, por ejemplo, por correo postal o electrónico.
- El software se instala en el dispositivo.

- Se introduce la clave de activación.
- Se selecciona e introduce un PIN (contraseña).

2. Inicio del software
- Se realiza cada vez que se inicia o reinicia el software.
- Introducción del PIN (contraseña).
- Uso de la funcionalidad del software (por ejemplo, banca en línea).
- Obtención, en caso necesario, de actualizaciones a través de un servidor de Internet (por ejemplo, un almacén o tienda de aplicaciones o App Store).

En comparación con soluciones conocidas con certificados de software, las formas de realización de la invención tienen la ventaja, entre otras, de que se pueden evitar ataques de fuerza bruta al servidor SSMS mediante la implementación de un contador de entradas de PIN incorrectas. A diferencia de los dispositivos en los que se utiliza el software, el servidor SSMS está protegido o securizado contra manipulaciones. En particular, el reinicio de dicho contador sólo es posible en el dispositivo, pero no en el servidor SSMS. Adicional o alternativamente, se puede definir en el servidor SSMS un tiempo de espera (que no puede ser manipulado por un atacante) que debe dejar que transcurra después de una entrada de contraseña incorrecta antes de que se pueda introducida una contraseña de nuevo, lo que hace que los ataques de fuerza bruta sean considerablemente más difíciles, por ejemplo del orden de unos pocos minutos u horas (por ejemplo, un tiempo de espera de al menos 5 o 10 minutos).

Además, la invención permite proteger los datos críticos. Esto se consigue en la forma de realización descrita anteriormente en el sentido de que la clave secreta y/o al menos partes del software son cifradas con una clave según el estándar AES, que es proporcionada por el servidor SSMS sólo en una sesión SSL existente. Por lo tanto, no es posible realizar ataques fuera de línea (por ejemplo, si el dispositivo es robado).

El software/aplicación puede, por ejemplo, comprender una serie de componentes que, o bien forman un paquete de software (por ejemplo, una aplicación que se puede descargar de un almacén o tienda de aplicaciones), o bien al menos en parte están presentes por separado. A modo de ejemplo, se puede proporcionar un programa de arranque o de carga no cifrado, que sirve para configurar el enlace con el servidor SSMS, realizar la autenticación en relación con el servidor SSMS y recibir la clave según el estándar AES procedente del servidor SSMS. Otro componente del software puede utilizar entonces para la comunicación real del dispositivo (por ejemplo, con otra unidad, tal como un servidor de banca en línea) y, para ello, puede ser cifrado con la clave según el estándar AES, de modo que sólo se puede utilizar después del descifrado. Este componente puede incluir, por ejemplo, un navegador que, por ejemplo, puede ser securizado. Por supuesto, este componente de comunicación también puede contener una interfaz gráfica de usuario y otros componentes necesarios para ejecutar la aplicación de comunicación real (por ejemplo, banca online), no sólo los componentes de comunicación puros. Otro componente del software puede estar destinado a realizar la fase de activación (véanse las Figuras 1 y 2) y estar presente sin cifrar para este fin. Cada uno o todos estos componentes del software pueden ser seguros o securizados.

Por ejemplo, los siguientes escenarios son concebibles:

1. Descargar una aplicación de inicio o de arranque no cifrada de un almacén o tienda de aplicaciones. Esto realiza el procedimiento de código de activación y recibe la clave según el estándar AES procedente del servidor SSMS y, si es necesario, también procedente de otro servidor, el programa de comunicación real que es cifrado con la clave según el estándar AES (en el servidor SSMS) o que será cifrado (en el dispositivo electrónico).

2. Descargar una aplicación completa (aplicación de inicio + programa de comunicación). La clave según el estándar AES es recibida usando la aplicación de arranque procedente del servidor SSMS y, de este modo, el programa de comunicación es cifrado individualmente.

El software se puede diseñar, en particular, como un software al menos parcialmente seguro; puede, por ejemplo, incluir un navegador seguro o securizado. A modo de ejemplo, se puede incluir una lista blanca de URL (una lista con sólo las URL que pueden ser accedidas). Adicional o alternativamente se puede utilizar sólo una página de inicio fija.

Se realiza un control de acceso de usuario cada vez que se inicia el software o programa. Cada vez que se inicia el programa, se podrá realizar un control de versiones y otros controles, por ejemplo, sobre la integridad del software y/o sobre el acoplamiento del software con el dispositivo correcto y/o sobre la necesidad de una actualización.

Opcionalmente, en formas de realización de la invención, se utiliza un componente de hardware. Esto puede, por ejemplo, en lugar del software/aplicación, almacenar una clave secreta/privada o permitir el acceso a la misma (si, por ejemplo, está almacenada en una tarjeta inteligente), pero por ejemplo, sólo cuando se introduce un PIN. Los componentes de hardware pueden tener, por ejemplo, una conexión cableada (por ejemplo, a través de un USB) o

inalámbrica (por ejemplo, a través de Bluetooth) con el dispositivo electrónico. En el caso de una comunicación Bluetooth, puede ser cifrada o no cifrada. En este caso, el componente de hardware puede ser recargable, por ejemplo, a través de un USB (incluso cuando la conexión es a través de Bluetooth).

El componente de hardware puede, por ejemplo, permitir una entrada segura del PIN, en especial si está diseñado como un lector de clase 3. A modo de ejemplo, un certificado SSL (por ejemplo, el certificado SSL utilizado en el contexto de la comunicación con el servidor SSMS) puede ser almacenado en una tarjeta inteligente certificada, que puede ser leída con el componente de hardware. La verificación de datos de la transacción se puede realizar en un display adicional (por ejemplo, del componente de hardware). El componente de hardware se puede utilizar para la implementación de una autenticación de dos factores (por ejemplo, tarjeta inteligente + PIN).

Los procedimientos de securización utilizados en las formas de realización de la invención son, por ejemplo, específicos para la respectiva plataforma subyacente (por ejemplo, iOS o Android en el caso de un teléfono inteligente). En este caso, por ejemplo, se pueden utilizar productos de securización externos (comerciales), por ejemplo, EnsureIT de Arxan o la solución Netheos.

Se puede utilizar un programa cargador relativamente pequeño y sin cifrar y luego el software real descifrado y cargado dinámicamente. Entonces, potencialmente, es posible la carga desde Internet. Sin embargo, es posible que no se permita la descarga de programas en algunas plataformas.

Los datos de configuración para el software/aplicación pueden, por ejemplo, almacenarse en una memoria persistente y, por lo tanto, protegerse contra la manipulación.

Se puede utilizar la ofuscación de código para proteger el software de la ingeniería inversa.

En formas de realización de la invención, se puede utilizar la invención para reemplazar el procedimiento mTAN establecido, con el canal de comunicación basado en SMS del procedimiento mTAN reemplazado por el canal de Internet basado en SSL de la presente invención. Esto puede servir como base para una matriz de seguridad, con la que los usuarios pueden decidir qué solución de seguridad es segura para el respectivo escenario de aplicación.

La Figura 3 muestra un ejemplo de escenario de aplicación de la invención. En este caso, el usuario interactúa con un dispositivo informático personal (PC) 6, en el que se utiliza un navegador seguro con certificados permanentes para banca por Internet (por ejemplo, para la autenticación del servidor bancario). El navegador seguro puede, por ejemplo, estar contenido en una partición de CD-ROM del PC 6 en forma preconfigurada y ser inalterable. En este caso, el PC 6 se comunica a través de un enlace conectado a través de SSL 8 con un servidor bancario (no mostrado).

El usuario también interactúa con un teléfono inteligente 7, en el que está instalado un software según la invención (por ejemplo, una aplicación (o App)). La aplicación está securizada y también está configurada para visualizar datos de transacción y números de transacción TAN. Se comunica a través de un enlace SSL 9 según ya se ha descrito en la Figura 2 con el servidor SSMS. Los números de transacción TAN pueden ser recibidos por varias rutas. A modo de ejemplo, el número de transacción TAN se puede recibir procedente del servidor SSMS (a través del enlace 9), una vez que el usuario del teléfono inteligente 7 ha realizado la auto autenticación en el servidor SSMS, ha recibido la clave según el estándar AES y, por lo tanto, ha descifrado los datos en el teléfono inteligente 7 (por ejemplo, partes del software/aplicación que son necesarias para obtener los números de transacción TAN y/o una clave secreta). Alternativamente, tras la autenticación en el servidor SSMS y la recepción de la clave según el estándar AES, se puede iniciar una comunicación con un servidor bancario (que puede ser idéntico o diferente del servidor bancario con el que se comunica el PC 6), por ejemplo, en base a parte del software, que sólo se puede descifrar con la clave según el estándar AES y/o una clave secreta (por ejemplo, para la autenticación en relación con el servidor bancario y/o para el cifrado de la comunicación con el mismo), que sólo se puede descifrar con la clave según el estándar AES.

El número de transacción TAN recibido de esta manera puede ser introducido por el usuario en el PC 6, con el fin de autorizar una acción bancaria en línea, tal como por ejemplo una remesa, que es iniciada con el navegador seguro o securizado.

La banca en línea en este ejemplo se basa, por lo tanto, en al menos dos canales separados. En primer lugar, el canal de comunicación basado en SSL 8 entre el PC y el servidor bancario, a través del cual se inician las transacciones, y en segundo lugar, el canal de comunicación basado en SSL 9 entre el teléfono inteligente y el servidor SSMS. El usuario funciona como el enlace entre los dos canales.

El canal de comunicación 9 entre el teléfono inteligente y el servidor SSMS o el servidor bancario, del que se obtiene el número de transacción TAN, toma entonces el rol de, por ejemplo, el canal mTAN basado en SMS convencional

10 que, sin embargo, puede ser atacado y comprometido por troyanos en el teléfono inteligente 7, que son capaces de escuchar y/o cambiar la comunicación SMS sin cifrar 10.

La Figura 4a muestra otro ejemplo de un escenario de aplicación de la invención, que se corresponde ampliamente con el escenario de la Figura 3. Sin embargo, a diferencia del escenario de la Figura 3, el PC 6' es un PC que no está totalmente controlado por el usuario. A modo de ejemplo, en el PC 6' sólo se puede utilizar un navegador no seguro para la banca en línea. Este puede, por ejemplo, ser el caso si el PC 6' se encuentra en un cibercafé. El canal de comunicación 8 del PC con el servidor bancario es entonces más fácil de romper que cuando se utiliza un navegador seguro (ver Figura 3). Sin embargo, como en el escenario de la Figura 3, la introducción de un canal de comunicación independiente 9 para transmitir los números de transacción TAN al usuario utilizando la aplicación segura o securizada, que se comunica con el servidor SSMS y sólo después de una autenticación satisfactoria en relación con el servidor SSMS, por ejemplo, permite que la aplicación se utilice para recibir los números de transacción TAN, contribuye a un aumento de la seguridad.

La Figura 4b muestra un escenario de aplicación adicional de la presente invención. La Figura 4b se refiere a una solución de autenticación fuera de banda para un acceso basado en PC a aplicaciones en línea. La solución de autenticación se puede utilizar, por ejemplo, para confirmar o rechazar inicios de sesión y/o transacciones (por ejemplo, remesas). Entre otras cosas, en este caso, se evitan debilidades y altos costes de las soluciones de autenticación basadas en SMS, así como debilidades y la susceptibilidad al error de contraseñas software de un solo uso (OTP) generadas en los dispositivos móviles como solución de autenticación.

En el escenario de la Figura 4b un usuario interactúa con un teléfono inteligente 45, en el cual está instalado un software de acuerdo con la invención (por ejemplo una aplicación (App)). La aplicación es, por ejemplo, segura o securizada. Según se ha descrito anteriormente, la aplicación se puede, por ejemplo, descargar de un servidor de aplicaciones (no se muestra en la Figura 4b) y luego registrar en el servidor SSMS 43. El acceso a datos locales almacenados en el teléfono inteligente 45 (en particular una clave secreta) sólo es posible si el usuario del teléfono inteligente 45 ha realizado una auto autenticación en el servidor SSMS 43 (por ejemplo, introduciendo un PIN en el teléfono inteligente), tras lo cual se recibe en el teléfono inteligente 45 la clave según el estándar AES y se descifran al menos en parte los datos locales (por ejemplo, al menos la clave secreta) con la clave según el estándar AES (por ejemplo, por parte de la aplicación). La clave secreta se utiliza, por ejemplo, para firmar mensajes que envía el teléfono inteligente 45 al servidor SSMS 43. Entre el teléfono inteligente 45 y el servidor SSMS 43 hay preferiblemente un enlace seguro 46, por ejemplo un enlace SSL. Para establecer este enlace 46 también se puede recurrir igualmente a la clave secreta. A modo de ejemplo, cuando se establece o configura el enlace, se firma la información (por ejemplo, una petición procedente del servidor SSMS u otro, por ejemplo, información específica de sesión) con la clave secreta en el teléfono inteligente y luego se verifica en el servidor SSMS con la clave pública asociada.

El usuario también interactúa con un navegador (u otra aplicación, por ejemplo, un software de banca en línea) en un PC 40 (u otro teléfono inteligente), que está conectado a través de un enlace 42, por ejemplo un enlace SSL, con el servidor de un banco 41. A modo de ejemplo, se produce un inicio de sesión en el servidor 41 y/o se realiza una transacción con el servidor 41 a través del navegador o la aplicación en el PC 40. El usuario puede ahora autenticarse al iniciar sesión o realizar transacciones por medio de una comunicación fuera de banda en base a la aplicación del teléfono inteligente 45, según se describe a continuación.

Inicialmente el usuario inicia sesión, introduciendo su nombre de usuario y contraseña (o información de autenticación alternativa, tal como por ejemplo datos biométricos) en el PC 40, en el servidor 41, por ejemplo a través de un portal en línea proporcionado en el servidor 41 que permite servicios en línea.

El usuario o su inicio de sesión pueden ahora, por ejemplo, ser autenticados (en un canal fuera de banda separado) en el sentido de que el servidor 41 solicita del servidor SSMS 43, a través del enlace 44, que por su parte puede ser un enlace seguro, una confirmación de inicio de sesión. A continuación, el servidor SSMS 43 envía a través del enlace seguro 46 un mensaje seguro a la aplicación del teléfono inteligente 45. Entonces, la información es mostrada en el teléfono inteligente 45 al usuario en relación con su inicio de sesión en el servidor 41, por ejemplo, de la siguiente forma: "¿Realmente quieres iniciar sesión en el servicio X del servidor Y?". En el teléfono inteligente 45, el usuario puede confirmar o rechazar esta información (por ejemplo, por medio de un teclado o de reconocimiento de voz). La confirmación o rechazo del usuario se envía al servidor SSMS 43 (por ejemplo, firmado con la clave secreta), que devuelve la correspondiente información al servidor 41 y, por lo tanto, confirma o no confirma el inicio de sesión del usuario en el servidor 41.

Alternativamente, el servidor SSMS 43, cuando el servidor 41 le pide la confirmación de inicio de sesión, puede generar un código, por ejemplo un código de una sola vez (por ejemplo, un código corto, que por ejemplo tiene menos de 6, 5 o 4 dígitos, con el fin de simplificar la entrada posterior por parte del usuario), y enviarlo a través del enlace seguro 46 a la aplicación del teléfono inteligente 45. El código es mostrado al usuario en el teléfono

inteligente 45. Entonces, el usuario introduce este código, por ejemplo, a través del teclado del PC 40 (o, por ejemplo, a través de transmisión directa, por ejemplo, óptica, acústica o de radio, especialmente a través de un enlace NFC o Bluetooth) en el PC 40, el cual envía entonces esta información al servidor 41 a través del enlace 42. El servidor 41 envía entonces el código a través del enlace 44 al servidor SSMS 43 para verificación. Si el código recibido procedente del servidor 41 coincide o se corresponde con el código enviado al teléfono inteligente 45, se ha confirmado (adicionalmente) el inicio de sesión del usuario en el servidor 41, y el servidor SSMS 43 y el servidor 41 pueden suministrar información correspondiente. De lo contrario, no ha sido satisfactoria la autenticación (posterior) del usuario.

En ambos procesos mencionados anteriormente de autenticación adicional del usuario, una condición para la transmisión de mensajes entre el servidor SSMS 43 y la aplicación del teléfono inteligente 45 es que el usuario del teléfono inteligente 45 haya realizado una auto autenticación en el servidor SSMS 43 (por ejemplo, introduciendo su PIN en el teléfono inteligente 45) y, por lo tanto, haya descifrado la clave secreta almacenada en el teléfono inteligente 45 de modo que pueda ser utilizada para la transmisión segura de datos con el servidor SSMS 43.

De forma similar a lo descrito para el proceso de inicio de sesión del usuario en el servidor 41 (a través del PC 40), las transacciones que el usuario realiza a través del PC 40 en el servidor 41 también pueden ser confirmadas a través del canal fuera de banda independiente que está formado por el servidor SSMS 43 y la aplicación del teléfono inteligente 45, por ejemplo mostrando información en el teléfono inteligente 45, por medio de la cual se solicita al usuario que confirme o rechace una transacción realizada en el servidor 41 a través del PC 40, o enviando un código desde el servidor SSMS 43 a la aplicación del teléfono inteligente 45, que debe ser introducido por el usuario en el PC 40 o enviado de otro modo por el teléfono inteligente 45 al PC 40, con el fin de confirmar la transacción. En este caso, el código puede, por ejemplo, representar el número de transacción (como en el ejemplo de las Figuras 3 y 4a), o puede ser necesario además de un número de transacción, que por ejemplo ha sido enviado al usuario a través de otra ruta (es decir, no a través del enlace 46).

La visualización de información procedente del servidor SSMS 43 en una unidad de visualización o display del teléfono inteligente 45 se puede realizar, por ejemplo, por medio de un software de visualización seguro y/o securizado, que es proporcionado o, al menos, controlado por la aplicación del teléfono inteligente. A modo de ejemplo, se puede utilizar la funcionalidad de visualización (por ejemplo, el componente Web View de un sistema operativo Android) de un navegador que (ya) está instalado en el teléfono inteligente 45.

La Figura 5a muestra otro ejemplo de escenario de aplicación de la invención. En este caso, el teléfono inteligente 7', en el que se instala la aplicación según la invención, se utiliza directamente para banca en línea (sin un PC 6/6' adicional como en las Figuras 3 y 4). Para ello, la aplicación contiene, por ejemplo, un navegador securizado para la comunicación (a través del enlace SSL 11) con el servidor bancario y también está configurado para la interacción (también a través del enlace SSL 11 o de un enlace SSL adicional) con el servidor SSMS, según se ha descrito en relación con la Figura 2.

La Figura 5a muestra otro componente de hardware opcional 12 para realizar una autenticación de dos factores, que a modo de ejemplo se conecta vía Bluetooth al teléfono inteligente 7' y puede acceder a una tarjeta inteligente (smartcard) certificada. La tarjeta inteligente (smartcard) puede, por ejemplo, almacenar (por ejemplo, en lugar del dispositivo 7' o del software/aplicación) la clave privada/secreta (o generarla) y/o utilizarla en conexión con la autenticación en relación con el servidor SSMS, aumentando así aún más la seguridad (en comparación con el uso de una contraseña). El componente de hardware 12 también puede incluir un display para visualizar información (por ejemplo, datos de transacción y/o números de operación).

La Figura 5b muestra otro escenario de aplicación de la presente invención que aumenta la fiabilidad de las acciones realizadas en terminales móviles (como, por ejemplo, procedimientos de inicio de sesión o transacciones). Todos los ataques actuales a los navegadores que se ejecutan en PC también pueden dirigirse a los navegadores que se ejecutan en terminales móviles, en particular teléfonos inteligentes. A modo de ejemplo, los usuarios pueden ser engañados por ataques de phishing o pharming cuando acceden a sus servicios en línea, o se pueden utilizar ataques de intermediario o de intermediario en navegador con el fin de alterar las acciones del usuario durante la ejecución de los mismos. En este caso, el uso convencional de contraseñas estáticas, SMS o contraseñas software de un solo uso (OTP) generadas en el terminal móvil no ofrece suficiente protección.

En la forma de realización de la Figura 5b, un usuario interactúa con un teléfono inteligente 50, en el que está instalado el software 52 de acuerdo con la invención (por ejemplo, una aplicación (App)). La aplicación 52 es, por ejemplo, segura o está securizada. Según se ha descrito anteriormente, la aplicación 52 puede, por ejemplo, ser descargada de un servidor de aplicaciones (no se muestra en la Figura 5b) y luego ser registrada en el servidor SSMS 55. El acceso a los datos locales almacenados en el teléfono inteligente 50 (en particular una clave secreta) sólo es posible si el usuario del teléfono inteligente 50 ha realizado la auto autenticación en el servidor SSMS 55 (por ejemplo, introduciendo un PIN en el teléfono inteligente 50), tras lo cual se recibiría la clave según el estándar AES

en el teléfono inteligente 50 y se descifrarían al menos parcialmente los datos locales (por ejemplo, al menos la clave secreta) con la clave según el estándar AES (por ejemplo, mediante la aplicación 52). La clave secreta se utiliza, por ejemplo, para firmar mensajes enviados por el teléfono inteligente 50 al servidor SSMS 55 y/o para configurar o establecer un enlace seguro, por ejemplo un enlace SSL, entre la aplicación 52 y el servidor SSMS 55. Con el fin establecer este enlace 57 también se puede utilizar la clave secreta, por ejemplo, para la autenticación en el lado del cliente, según se ha descrito anteriormente.

En la presente forma de realización, la aplicación 52 comprende un navegador 51. El navegador 51 puede ser un componente integral de la aplicación 52, o se puede ejecutar utilizando los recursos de un navegador instalado en el teléfono inteligente 50 independientemente de la aplicación 52 (por ejemplo, del navegador estándar del teléfono inteligente 50, que está preinstalado en el teléfono inteligente cuando es entregado). Por ejemplo, el navegador 51 puede tomar la forma de un componente Web View de un navegador instalado en el teléfono inteligente (por ejemplo, en un teléfono inteligente 50 con sistema operativo Android). Alternativamente la aplicación 52 también puede no contener su propio navegador 51 y en su lugar controlar un navegador del teléfono inteligente 50.

La aplicación 52 proporciona al teléfono inteligente 50, por ejemplo, unos mecanismos de seguridad que son específicos del navegador 51 y que, por ejemplo, controlan o restringen su uso al menos parcialmente. Estos mecanismos de seguridad pueden, por ejemplo, incluir una o más de las siguientes características:
- Un filtro de lista blanca de URL (Uniform Resource Locators), es decir, una lista de URL permitidas, que el usuario puede invocar con el navegador 51. Esto evita el acceso a sitios de Internet erróneos o falsos.
- Un almacén seguro de certificados (por ejemplo, accesible sólo a través de la aplicación) para certificados de autoridades de certificación de confianza (CA) para la verificación de certificados de servidor y para la protección de enlaces SSL. Esto puede, en particular, ser independiente del almacén de certificados del teléfono inteligente 50.
- Un display seguro integrado para mensajes auténticos (por ejemplo, procedentes del servidor SSMS) al usuario. Esta pantalla o display puede, por ejemplo, estar diseñada por desarrolladores de aplicaciones, por ejemplo, como un componente GUI, o por ejemplo, también utilizando el componente Web View de los navegadores 51 en el caso de un sistema operativo Android). El display estándar del navegador 51 no se utiliza para mostrar mensajes importantes (tal como, por ejemplo, información de inicio de sesión o información de transacción), sólo la pantalla segura. La visualización global de la aplicación puede incluir, por ejemplo, la visualización o display estándar del navegador 51 en una parte superior y el display seguro en una parte inferior a la misma.

La aplicación 52 puede, por ejemplo, estar adaptada a los requerimientos de un proveedor de servicios en línea, cuyos servicios son accesibles con el teléfono inteligente 50. Las partes adaptables constituyentes de la aplicación 52 comprenden, por ejemplo, uno o más de los siguientes componentes:
- Imágenes de fondo de la interfaz gráfica de usuario.
- Recursos de texto (por ejemplo, texto que visualiza o muestra la aplicación. A modo de ejemplo, de esta manera se pueden añadir otros idiomas o adaptar la terminología al uso lingüístico del respectivo cliente.)
- Una URL para la aplicación en línea estándar y un filtro de lista blanca de URL.
- Certificados SSL de la autoridad de certificación como anclaje de confianza.

Cuando un usuario utiliza la aplicación 52, se le pide que realice una auto autenticación en el teléfono inteligente 50 en relación con el servidor SSMS 55 (por ejemplo, introduciendo su PIN). A continuación, y según se ha descrito anteriormente, se verifica la información de entrada en el servidor SSMS 55 y se establece un enlace seguro 57 entre el servidor SSMS 55 y el teléfono inteligente 50 o la aplicación 52.

El proceso de inicio de sesión del usuario en el servidor 53 de un proveedor de servicios (en la Figura 5b, por ejemplo, se supone que es un banco) a través de una aplicación -en este caso, una página de Internet mostrada en el navegador 51- para iniciar sesión en el servidor 53 puede comenzar entonces, por ejemplo, en el momento en que el usuario introduce su nombre de usuario (por ejemplo, un ID) y, por ejemplo, una contraseña estática en el navegador 51 (por ejemplo, a través del teclado del teléfono inteligente 50). Estos datos se verifican en el servidor 53. A continuación, el servidor 53 solicita, a través del enlace 56, una autenticación adicional del usuario desde el servidor SSMS 55. El servidor SSMS 55 envía para este propósito a través del enlace seguro 57, configurado según se ha indicado anteriormente, un mensaje seguro a la aplicación 52 del teléfono inteligente 50. A continuación, en el teléfono inteligente 50 (por ejemplo, en el display seguro de la aplicación 52) se muestra al usuario información relativa a su inicio de sesión en el servidor 53, por ejemplo, de la siguiente forma: "¿Realmente quieres iniciar sesión en el servicio X del servidor Y?". El usuario puede confirmar o rechazar esta información en el teléfono inteligente 50 (por ejemplo, por medio del teclado o del reconocimiento de voz). La confirmación o rechazo del usuario se envía al servidor SSMS 55 (por ejemplo, en forma de mensaje firmado con la clave secreta), que devuelve correspondiente información al servidor 53 y confirma o no confirma el inicio de sesión del usuario en el servidor 53.

Alternativamente, la autenticación del usuario también se puede realizar sin necesidad de introducir el nombre de usuario y la contraseña en la aplicación (en este caso, a modo de ejemplo, una página de Internet mostrada en el navegador 51) para iniciar sesión en el servidor 53. Para ello, el servidor SSMS 55 (por ejemplo, en respuesta al

inicio de la aplicación 52 en el teléfono inteligente 50 y a la autenticación del usuario en relación con el servidor SSMS 55 a través de la aplicación 52) genera un código de una sola vez (el cual, por ejemplo, por razones de seguridad, puede ser relativamente largo (por ejemplo, con más de 8, 16 o 32 dígitos), ya que el usuario no tiene que introducirlo) y lo envía (por ejemplo, como un billete de entrada) a través del enlace seguro 57 a la aplicación 52. La aplicación 52 envía este código a la aplicación que se utiliza para iniciar sesión en el servidor 53, por ejemplo, automáticamente. A modo de ejemplo, el código es introducido automáticamente en una página de Internet que se muestra en un navegador 51 para iniciar sesión en el servidor 53. El código es enviado entonces por el servidor 53 a través del enlace 56 para verificación al servidor SSMS 55, que en caso de coincidencia entre el código generado y el código recibido procedente del servidor 53 devuelve información al servidor 53, de que el usuario ha realizado satisfactoriamente la auto autenticación (y por lo tanto puede utilizar el servicio del servidor 53). Dado que ya no es necesario que el usuario introduzca el nombre de usuario y la contraseña en la aplicación/navegador 51, se incrementa aún más la facilidad de uso en comparación con las variantes descritas anteriormente. La autenticación del usuario en relación con el servidor 53 se basa en este caso, por lo tanto, en la entrada del PIN por parte del usuario para el servidor SSMS 55 (y opcionalmente una comprobación de si la aplicación 52 se ha registrado correctamente en el servidor SSMS 55 y/o está intacta y/o está instalada en el teléfono inteligente 50 correcto).

De la misma manera que se describe para el proceso de inicio de sesión del usuario en el servidor 53, las transacciones que el usuario realiza a través del navegador 51 en el servidor 53, pueden ser autenticadas además a través del canal fuera de banda independiente que está formado por el servidor SSMS 55 y la aplicación 52 del teléfono inteligente 50, de este modo a través, por ejemplo, de la visualización de información en el teléfono inteligente 50, por medio de la cual se pide al usuario que confirme o rechace una transacción realizada en el servidor 53 a través del navegador 51, o enviando un código desde el servidor SSMS 55 a la aplicación 52 del teléfono inteligente 50, que es enviado luego desde la aplicación 52 a la aplicación/navegador 51 (en este caso también se puede prescindir de forma ventajosa de la entrada manual del código en la aplicación por parte del usuario). En este caso, el código puede, por ejemplo, representar el número de transacción (como en el ejemplo de las Figuras 3 y 4a), o puede ser necesario adicionalmente a un número de transacción, que por ejemplo ha sido enviado al usuario a través de otra vía o ruta (por lo tanto, no a través del enlace 57).

La apariencia del software según la invención/aplicación (por ejemplo, la interfaz de usuario) se puede, por ejemplo, adaptar o alterar con la ayuda de una interfaz de configuración (por ejemplo, una interfaz de configuración genérica), con el fin de permitir, por ejemplo, la generación de marcas para diferentes bancos.

Alternativamente, según la invención, se puede proporcionar un SDK (kit de desarrollo de software) de comunicaciones y seguridad para crear el software según la invención/aplicación, en el que la interfaz de usuario del software/aplicación puede entonces ser definida individualmente por parte de los usuarios del kit SDK (por ejemplo, programador de aplicaciones para diversos bancos).

Como alternativa adicional, el software/aplicación se puede configurar de forma que el servidor SSMS u otro servidor cargue una máscara (denominada "piel") que determina el aspecto de la interfaz de usuario durante la fase de activación/inicialización (véanse las Figuras 1 y 2) y luego vinculada con el software/aplicación. Si el software/aplicación se vende a través de una tienda de aplicaciones, entonces el software/aplicación siempre se podrá obtener en esta tienda con el mismo nombre, ya que la adaptación específica del banco sólo se realiza después de una descarga satisfactoria durante la fase de activación/inicialización.

Formas de realización de la invención permiten (por ejemplo, a diferencia del procedimiento convencional de símbolos de software) el uso de un contador para los intentos fallidos de autenticación (por ejemplo, entradas de contraseña incorrectas) en el servidor SSMS (por lo tanto, en un entorno más seguro que el dispositivo), de modo que los ataques de fuerza bruta son imposibles y también se pueden utilizar contraseñas más sencillas. Las contraseñas simples se utilizan sobre todo en los dispositivos móviles, ya que, debido a sus pequeños teclados, hacen que la introducción de contraseñas complejas lleve mucho tiempo. Además, los datos locales del software están cifrados en el dispositivo, de modo que malware en el dispositivo no puede leer ningún dato secreto (no cifrado).

Si el dispositivo es robado temporalmente y su contenido es copiado, cualquier atacante se enfrenta al obstáculo adicional de que se tienen que verificar cualesquiera valores de hardware que puedan estar en el software securizado.

El requisito de iniciar sesión en el servidor SSMS para cada acción permite, entre otras cosas, una comprobación regular de la versión del software y la imposición de actualizaciones. A modo de ejemplo, la realización de operaciones bancarias en línea puede ser prohibida si se considera que la versión del software está desactualizada.

Si el software según la invención es diseñado como una aplicación, que se instala en un teléfono inteligente y se obtiene a través de una tienda de aplicaciones (App Store), se pueden utilizar de forma ventajosa varios mecanismos de seguridad del proveedor del teléfono inteligente, por ejemplo:
- Se comprueban las aplicaciones antes de incluirlas en el almacén o tienda de aplicaciones, por ejemplo, para comprobar su compatibilidad (por ejemplo, con Apple).
- Está prohibida la instalación de aplicaciones desconocidas (y por lo tanto no procedentes de la tienda de aplicaciones) en el teléfono inteligente.
- Las aplicaciones con malware se pueden eliminar de forma remota desde los dispositivos.
- Los sistemas operativos de los teléfonos inteligentes proporcionan las denominadas sandboxes, y las aplicaciones no pueden interactuar entre sí.

Según se ha explicado anteriormente, en formas de realización de la invención se puede utilizar una clave secreta/privada (en adelante también denominada "clave privada") para autenticación, firma y/o cifrado de la comunicación del dispositivo con otra unidad, por ejemplo, con un servidor bancario. Esta clave se puede almacenar en diversos puntos, según se describe con más detalle a continuación. Lo que es común a todos los escenarios, sin embargo, es que el acceso a la clave (completa) y, por lo tanto, su uso sólo es posible tras una autenticación satisfactoria con el servidor SSMS. En la siguiente descripción de las Figuras 6-8, se utiliza la clave (completa) para la autenticación en relación con un servidor bancario. Sin embargo, la clave secreta también se puede utilizar alternativamente para la autenticación en relación con el servidor SSMS (por ejemplo, cuando se establece un enlace seguro, tal como por ejemplo un enlace SSL/TLS o para la firma de mensajes al servidor SSMS), según ya se ha descrito de forma exhaustiva.

La clave privada/secreta 18 puede, según se muestra en la Figura 6, almacenarse en el software/aplicación 13'. De este modo, la clave 18 es cifrada simétricamente junto con el software 13' para obtener el software 13. El acceso al software 13' y también a la clave privada 18 sólo es posible entonces tras la autenticación satisfactoria con el servidor SSMS 14 (mediante la contraseña 16) y la recepción de la clave según el estándar AES 17 (para descifrar el software 13). La clave privada/secreta 18 se utiliza entonces en la comunicación con el servidor bancario 15 (o el servidor SSMS) (por ejemplo, para la autenticación en el lado del cliente en el contexto del enlace SSL/TLS, según se describe, por ejemplo, en el contexto de la Figura 2). Alternativamente, por supuesto, sólo se puede cifrar simétricamente la clave 18, pero no el software 13'. Entonces, el acceso a la clave 18 depende de la obtención de la clave según el estándar AES 17.

La clave privada/secreta 18a/18b también puede, según se muestra a modo de ejemplo en la Figura 7, almacenarse de manera distribuida, y de hecho como parte 18a en el servidor SSMS y como parte 18b en el software/aplicación 13'. Tanto el servidor SSMS 14 como el software 13' deben utilizar su parte de la clave 18a/18b, de modo que se obtiene una firma válida que se puede comprobar utilizando procedimientos convencionales. Esto ofrece seguridad incluso si el software 13' es robado o pirateado. El administrador del servidor SSMS 14 no puede realizar ningún ataque con la clave parcial 18a, el software 13' o la clave 18b contenida en el mismo debe estar siempre involucrado (y también el software 13' descifrado). En este caso, también alternativamente se puede cifrar simétricamente sólo la parte 18b de la clave, pero no el software 13'. El acceso a la parte 18b depende entonces de la obtención de la clave según el estándar AES 17 y además se requiere la parte 18a de la clave.

A continuación se explica el principio de la clave privada/secreta distribuida 18a/18b o la firma asociada para el ejemplo de una firma RSA.

Firma: $Text^{privKey} = Sig$

(La firma sig se obtiene, de este modo, a partir de un texto mediante la aplicación de la clave privada privKey, por ejemplo, mediante el cifrado de un valor hash del texto).

Verificación: $Sig^{pubKey} = Texto$

(La verificación se produce mediante la aplicación de la clave pública pubKey a la firma recibida, por ejemplo descifrando el valor hash del texto, recreando el valor hash a través del texto y comparando los dos valores hash).

En términos simplificados privKey = 1/pubKey.

Por lo tanto, la firma también se puede calcular independientemente de la siguiente manera, en el sentido de que la privKey puede dividirse en varios sumandos:

privKey= privKey1 + privKey2.

Esto produce lo siguiente:

Firma: $Text^{privKey} = Text^{privKey1+privKey2} = Text^{privKey1} * Text^{privKey2}$

Esto significa que se pueden calcular independientemente dos partes de la firma que se multiplican entre sí para obtener una firma RSA. Esto se puede comprobar de la manera convencional.

Los sumandos de la clave se pueden almacenar en el servidor SSMS 14, el software 13' y/o el hardware de forma distribuida, con el fin de aumentar la seguridad.

Según se muestra en la Figura 7, durante la autenticación en relación con el servidor bancario 15 se utilizan de este modo dos piezas de información de autenticación (por ejemplo, información firmada), de las cuales una primera se genera en el software 13' con la primera parte de la clave RSA (privKey1) y se transmite al servidor SSMS 14, y la segunda se genera en el servidor SSMS 14 con la segunda parte de la clave RSA (privKey2) y se multiplica con la primera información de autenticación, con el fin de obtener la información de autenticación completa. A continuación, el servidor SSMS la devuelve al software 13' y puede utilizarla para la autenticación en relación con el servidor bancario 15, por ejemplo, cuando se establece o configura un enlace SSL/TLS con autenticación en el lado del cliente y en el lado del servidor de acuerdo con la RFC 5246.

Se citan a modo de ejemplo las siguientes referencias a la literatura sobre la firma RSA distribuida:

1) D. Boneh, M. Franklin, Efficient Generation of Shared RSA keys, Konferenzband Advances in Kryptology - Crypto 97, LNCS 1294 S. 425-439 35

2) J. Benaloh (Cohen), Secret sharing homomorphiSMS: keeping shares of a secret, Crypto 86, S.251-260

3) M. Ben-Or, S. Goldwasser, A. Widgerson Completeness theorems for non-cryptographic fault tolerant distributed computation STOC 1988, S.1-10

4) M. Malkin, Th.Wu und D. Boneh, Experimenting with Shared Generation of RSA keys, Konferenzband Internet Societys 1999 Symposium on Network and Distributed System Security (sNDSS), S. 43-56.

Por último, la clave privada/secreta 18 también se puede almacenar completamente en el servidor SSMS 14, según se muestra en la Figura 8, y en este caso también sólo puede accederse a la clave 18 tras la autenticación en el servidor SSMS 14 y la recepción de la clave según el estándar AES 17, por ejemplo porque la comunicación con el servidor SSMS y/o el acceso a la clave 18 almacenada en el servidor SSMS sólo es posible con el software descifrado 13'. A modo de ejemplo, la clave 18 se puede cifrar con una clave (por ejemplo simétrica), que se almacena en el software descifrado 13'. De esta manera se puede evitar el acceso (malicioso) de un administrador del servidor SSMS 14 a la clave 18. De este modo, la clave 18 se almacena en el servidor SSMS 14. Los ataques al software 13' no pueden comprometerla.

Según ya se ha descrito generalmente antes, con el fin de aumentar la seguridad se puede utilizar un componente de hardware adicional (por ejemplo, el componente 12 de la Figura 5) que, por ejemplo, se conecta al dispositivo/teléfono inteligente a través de Bluetooth (u otra conexión inalámbrica o cableada, por ejemplo, a través de comunicación de campo cercano (NFC) o a través de un enlace acústico u óptico). Este componente de hardware puede, por ejemplo, almacenar (en lugar del dispositivo o del software/aplicación) la clave privada/secreta (por ejemplo, una clave RSA) de forma que no pueda ser leída. La clave puede ser utilizada únicamente por el componente de hardware. Los algoritmos criptográficos necesarios (por ejemplo, el cálculo de firmas) son calculados en el componente de hardware. Puede tratarse de una tarjeta inteligente (smartcard) + un terminal de tarjeta u otro componente de hardware. La clave secreta puede (por ejemplo, en la fase de inicialización), por ejemplo, ser generada en el dispositivo/teléfono inteligente y escrita en el hardware, o puede ser generada en el propio hardware. Una correspondiente clave pública puede, en el último caso por ejemplo, ser exportable desde el hardware, por ejemplo, al dispositivo/teléfono inteligente o al servidor SSMS.

El componente de hardware adicional crea un obstáculo mayor para un atacante, porque debe controlar tanto el software/aplicación o el dispositivo/teléfono inteligente, como el componente de hardware.

En este caso nuevamente se pueden identificar varios escenarios posibles relacionados con la entrada y el almacenamiento del PIN, perteneciente a la tarjeta inteligente (smartcard), los cuales se describen a continuación. Sin el PIN, por ejemplo, no es posible acceder a la clave privada/secreta de la tarjeta inteligente (smartcard) o del propio componente de hardware, ni utilizarla.

1. El PIN es introducido en el software/aplicación o es almacenado en el mismo.

En este caso, por ejemplo, el PIN puede introducirse cada vez a través del software y no almacenarse o introducirse sólo una vez a través del software y almacenarse en el software/aplicación para su reutilización. El PIN puede, por ejemplo, cifrarse con la clave según el estándar AES (o también con la clave secreta/privada del software, que también puede estar presente de forma distribuida según se describe en la Figura 7) y almacenarse en el dispositivo, por ejemplo como un componente del software, pero alternativamente también de forma independiente del mismo. Sin interacción con el servidor SSMS, por lo tanto, es bastante imposible el uso de la clave de hardware externa -por ejemplo, en el caso de que un atacante no esté usando el software, sino que esté escribiendo su propio software/aplicación, que busca acceder al hardware directamente.

Si se va a realizar una autenticación en relación con un servidor bancario o el servidor SSMS (según se ha descrito, por ejemplo, en las Figuras 2 y 6), la información (por ejemplo, en relación con la autenticación en el lado del cliente) que debe ser firmada y/o cifrada puede ser enviada por el software al componente de hardware y después de una comprobación del PIN descifrado en el software y mostrada al componente de hardware firmado/cifrado. Si el software/aplicación y el componente de hardware están acoplados, el componente de hardware no ofrece protección adicional. Sin embargo, en este caso, la clave privada puede ser leída.

2. Se introduce el PIN cada vez en el componente de hardware.

En este caso hay un nivel muy alto de protección de la clave privada. Debido a que es necesario introducir el PIN en el componente de hardware, prácticamente no hay posibilidad de ataque. Sin embargo, hay un cierto esfuerzo por parte del usuario, que en este caso debe introducir tanto la contraseña/código de acceso para el software/aplicación como el PIN en el componente de hardware. El software cifrado con la clave según el estándar AES en el dispositivo puede ser diseñado para aumentar la seguridad de tal manera que la comunicación con el componente de hardware o el acceso a dicho componente de hardware sólo sea posible a través del software descifrado, por ejemplo, mediante una función de autenticación especial almacenada en el software (que puede ser diferente del PIN de Smartcard).

3. El servidor SSMS almacena el PIN y lo envía al componente de hardware a través del software/aplicación.

En este caso se puede utilizar un canal cifrado entre el software/aplicación y el servidor SSMS y/o un canal cifrado entre el componente de hardware y el servidor SSMS. Preferiblemente ambos canales son cifrados.

Este es un procedimiento conveniente y seguro si el PIN es enviado por el servidor SSMS a través de un canal seguro al componente de hardware (mensajería segura entre el servidor SSMS y el componente de hardware). El PIN debe almacenarse preferiblemente en el servidor SSMS cifrado (por ejemplo, en base a una clave (por ejemplo, simétrica), que se almacena en el software del dispositivo, que a su vez sólo se puede descifrar con la clave según el estándar AES procedente del servidor SSMS). Para un ataque, los PIN deben ser extraídos del servidor SSMS y se deben robar las tarjetas inteligentes asociadas.

4. El servidor SSMS envía al menos una parte del PIN y se introduce una parte (a través del software o en el componente de hardware).

Esta variante ofrece la mayor seguridad. Una tarjeta inteligente (smartcard) robada no se puede utilizar sin el servidor SSMS, pero incluso con los datos del PIN procedentes del servidor SSMS un ataque sólo tiene unas pocas posibilidades de éxito. La parte del PIN almacenada en el servidor SSMS puede, en este caso, a su vez, ser cifrada con una clave (por ejemplo simétrica), que se almacena en el software del dispositivo, que a su vez puede ser descifrada sólo con la clave según el estándar AES procedente del servidor SSMS.

La Figura 9 es una representación esquemática de los componentes de una forma de realización de un dispositivo electrónico según la invención. El dispositivo electrónico puede ser, por ejemplo, un teléfono inteligente, por ejemplo, el teléfono inteligente de las Figuras 1, 3, 4a, 4b, 5a y 5b. El dispositivo comprende un procesador 90, que controla una unidad de visualización o display 93 (por ejemplo, un LCD, por ejemplo, para producir una o más displays que incluyen un display seguro), un teclado 94 y una interfaz de comunicaciones 95. La interfaz de comunicaciones permite la comunicación entre el dispositivo y otras entidades (por ejemplo, con el servidor SSMS y/o el servidor de un proveedor de servicios y/o un hardware externo como, por ejemplo, un lector de tarjetas inteligentes), por ejemplo, a través de enlaces inalámbricos o cableados. El procesador 90 ejecuta uno o más programas, que se almacenan en la memoria de programas 91 (por ejemplo, una memoria flash). Esto puede implicar un sistema operativo y otros programas - en particular el software según la invención. Por ejemplo, el software está configurado para enviar información de autenticación al servidor SSMS, recibir la primera clave procedente del servidor SSMS, descifrar la información cifrada almacenada en el dispositivo electrónico con la primera clave y utilizar esta información descifrada en una comunicación, por ejemplo, con el servidor SSMS o con otro servidor según ya se ha descrito ampliamente. Con el fin de ejecutar los programas, el procesador 90 utiliza la memoria de trabajo 92, que por ejemplo puede ser diseñada como una memoria RAM. El almacén de certificados del software según la

invención puede, por ejemplo, ser almacenado en la memoria de programas 91 (u otra memoria persistente). La clave secreta cifrada del software según la invención se puede almacenar, por ejemplo, en la memoria de programas 91 (u otra memoria persistente).

La Figura 10 es una representación esquemática de los componentes de una forma de realización de un servidor según la invención. El servidor puede ser, por ejemplo, el servidor SSMS de las Figuras 1, 2, 4b, 5b, 6, 7 y 8. Básicamente, sin embargo, el servidor de un proveedor de servicios (por ejemplo, un banco) también puede tener una estructura de este tipo. El servidor comprende un procesador 100 que controla una interfaz de comunicaciones 103. La interfaz de comunicaciones permite la comunicación entre el servidor y otras entidades, por ejemplo con otros servidores y/o con el dispositivo electrónico según la invención, por ejemplo a través de un enlace SSL o TLS. El procesador 100 ejecuta uno o más programas, que se almacenan en la memoria de programas 101 (por ejemplo, una memoria flash). Esto puede implicar un sistema operativo y otros programas, en particular programas informáticos para establecer un enlace con el dispositivo electrónico, autenticar al usuario del dispositivo electrónico y/o del dispositivo electrónico y suministrar una primera clave en caso de que la autenticación tenga éxito. En este caso, el suministro de la primera clave puede depender, según ya se ha descrito, de la realización de comprobaciones adicionales en relación con el software del dispositivo electrónico, por ejemplo, en lo que se refiere a la integridad, la versión y/o el enlace o vinculación del software con el dispositivo electrónico correcto. El software también puede ser configurado para la comunicación con el dispositivo electrónico de acuerdo con la invención, por ejemplo para establecer un enlace seguro con el dispositivo electrónico, para enviar información sobre un procedimiento de inicio de sesión y/o transacción que debe ser confirmado o rechazado por un usuario del dispositivo electrónico y para recibir información firmada (por ejemplo, relativa a la confirmación/rechazo del procedimiento de inicio de sesión y/o transacción) procedente del dispositivo electrónico. El software también puede ser configurado para la comunicación con el servidor de un proveedor de servicios, en el que el usuario del dispositivo electrónico realiza procedimientos de inicio de sesión y/o transacción, por ejemplo, para responder positivamente a preguntas de autenticación procedentes de este servidor y para suministrar confirmaciones o rechazos de autenticación al servidor. Para ejecutar los programas, el procesador 100 utiliza la memoria de trabajo 102 que, por ejemplo, puede ser diseñada como una memoria RAM.

La Figura 11 es una representación esquemática de una forma de realización de un medio de almacenamiento 1100 según la invención. El medio de almacenamiento 1100 almacena un programa 1101, que a su vez contiene un código de programa 1102. El programa puede ser, por ejemplo, el software según la invención ejecutado en el dispositivo electrónico o el software según la invención ejecutado en el servidor. El medio de almacenamiento 1100 puede representar, por ejemplo, la memoria de programas 91 de la Figura 9 o la memoria de programas 101 de la Figura 10. El medio de almacenamiento 1100 puede, por ejemplo, almacenar también el kit de desarrollo de programas informáticos según la invención.

La invención se ha descrito usando ejemplos de formas de realización. Sin embargo, la invención no se limita a estas formas de realización específicas. En particular, la invención se puede utilizar no sólo en el ámbito de la banca en línea, sino también, por ejemplo, en otros escenarios en los que se requiera una autenticación segura y/o una comunicación cifrada, por ejemplo, para el acceso remoto a datos o para el control remoto de instalaciones o maquinaria.

Ejemplos de áreas de aplicación de la invención son:

- En el sector bancario:
  - o Garantizar la seguridad de los procedimientos de inicio de sesión y/o de transacción en banca en línea y en banca móvil.
  - o Autenticación durante pagos en línea, cuando la tarjeta de crédito o débito no está presente. Los bancos suelen utilizar PIN estáticos o contraseñas de un solo uso en SMS para la denominada autenticación 3D (autenticación segura 3D). Estas soluciones son relativamente débiles, y los usuarios no tienen forma de mostrar y verificar los detalles de la transacción de manera segura. La presente invención puede ser integrada en la autenticación 3D y los detalles de la transacción (a través del servidor SSMS) enviados al usuario para su confirmación.
  - o Autenticación para retiradas de efectivo en cajeros automáticos. Estas autenticaciones pueden ser permitidas (por el servidor SSMS), aunque no haya tarjeta de débito presente, es decir, mediante la confirmación de una retirada de un cajero automático en un móvil por parte del usuario.
- En el sector de los juegos en línea: en la actualidad, los juegos están muy extendidos en Internet. Algunos juegos requieren un inicio de sesión, en el que los usuarios pueden compartir contraseñas. Para algunos juegos gratuitos, sin embargo, los usuarios pueden querer proteger su perfil de juego y no permitir a otros la posibilidad de acceder a sus cuentas con contraseñas estáticas robadas. Una vez más, este requisito puede ser satisfecho por la presente invención, en el sentido de que el procedimiento de inicio de sesión de un usuario es además confirmado a través del servidor SSMS.
- En aplicaciones Web online de empresas, por ejemplo sistemas CRM (Customer Relationship Management – gestión de relaciones con clientes), sistemas ERP (Enterprise Resource Planning – planificación de recursos de empresa), sistemas de correo electrónico (por ejemplo, acceso web Outlook). En este caso, el servidor SSMS puede

confirmar el inicio de sesión del usuario (y posiblemente también acciones después del procedimiento de inicio de sesión).
- En VPN (Virtual Private Networks – Redes Privadas Virtuales) – acceso, por ejemplo a través de SSL. El enlace SSL puede ser establecido o configurado, por ejemplo, en base a un certificado, que sólo puede ser descifrado en el terminal móvil una vez que el usuario ha sido autenticado en el servidor SSMS.
- En aplicaciones en línea en el ámbito de la asistencia sanitaria, por ejemplo, en el acceso electrónico a los historiales médicos. En este caso, también se puede realizar una autenticación adicional de un usuario a través del servidor SSMS.
- En juegos de apuestas online. En este caso, también es necesaria la protección tanto de los usuarios como de los proveedores de servicios, lo que puede garantizarse por medio de una autenticación adicional por parte del servidor SSMS.

La secuencia de las etapas de proceso descritas en esta especificación no es obligatoria, son concebibles secuencias alternativas de las etapas de proceso. Las etapas del proceso pueden ser implementadas de varias maneras, por lo que son concebibles una implementación en software (a través de instrucciones de programa), en hardware o una combinación de las mismas para la implementación de las etapas del proceso.

Las formas de realización de ejemplo de la presente invención descritas en esta especificación también se consideran divulgadas en todas las combinaciones entre las mismas. En particular, también la descripción de una característica de una forma de realización – a menos que se indique expresamente lo contrario - no se entenderá que signifique en este caso que la característica es indispensable o esencial para el funcionamiento de la forma de realización.

REIVINDICACIONES

1. Procedimiento realizado en un dispositivo electrónico (3) que está conectado comunicativamente a un servidor (2), comprendiendo el procedimiento:
- autenticar al usuario del dispositivo electrónico (3) y/o al dispositivo electrónico con el servidor (2),
- proporcionar una primera clave procedente del servidor (2) tras una autenticación satisfactoria;
- descifrar datos cifrados almacenados en el dispositivo electrónico (3) con la primera clave mediante un software almacenado en el dispositivo electrónico (3);
- realizar una comunicación del dispositivo electrónico (3) utilizando los datos descifrados, o
- realizar una comunicación del dispositivo electrónico (3) utilizando la primera clave junto con datos almacenados en el dispositivo electrónico (3);
en el que la primera clave no se almacena de forma permanente en el dispositivo electrónico,
caracterizado en que
el procedimiento es ejecutado y/o controlado por el software almacenado en el dispositivo electrónico (3), y en el que el servidor (2) comprueba al menos una característica del software y al menos una característica del dispositivo electrónico (3) durante la autenticación con el servidor (2) y sólo se obtiene la primera clave si la comprobación ha sido satisfactoria.

2. Procedimiento según la reivindicación 1, comprendiendo el procedimiento además en una fase de inicialización:
- obtener datos cifrados que están cifrados con la primera clave; y
- almacenar los datos cifrados en el dispositivo electrónico (3).

3. Procedimiento según una de las reivindicaciones 1 a 2, en el que la primera clave es una clave única de usuario, y en el que la primera clave es generable por el servidor (2) durante una fase de inicialización.

4. Procedimiento según una de las reivindicaciones 1 a 3, en el que al menos una característica del software representa su integridad con respecto a un estado original o a un estado derivable del mismo mediante actualizaciones oficiales.

5. Procedimiento según una de las reivindicaciones 1 a 4, en el que los datos descifrados que comprenden un software para comunicación del dispositivo electrónico (3) y/o al menos parte de una segunda clave para autenticación del dispositivo electrónico (3) y/o del usuario del dispositivo electrónico (3) y/o para cifrar la comunicación del dispositivo electrónico (3) y/o para firmar mensajes del dispositivo electrónico (3).

6. Procedimiento según la reivindicación 5, comprendiendo el procedimiento además en una fase de inicialización:
- generar la segunda clave en el dispositivo electrónico (3).

7. Procedimiento según una de las reivindicaciones 1 a 6, en el que la comunicación requiere la autenticación del dispositivo electrónico (3) y/o la autenticación de un usuario del dispositivo electrónico (3), y en el que los datos descifrados contienen al menos parte de la información necesaria para la autenticación requerida por la comunicación o son necesarios para el uso de al menos parte de esta información.

8. Procedimiento según una de las reivindicaciones 1 a 7, en el que los datos descifrados contienen al menos una parte de un software y/o información necesaria para obtener información de autenticación almacenada en el servidor (2) y/o en el que los datos descifrados contienen al menos una parte de un software y/o información necesaria para usar información de autenticación que puede ser accedida por un dispositivo (12) conectable al dispositivo electrónico (3).

9. Procedimiento según una de las reivindicaciones 1 a 8, en el que se realiza la comunicación entre el dispositivo electrónico y el servidor y sirve para autenticar al usuario en operaciones de inicio de sesión y/o transacción realizadas por el usuario del dispositivo electrónico con el dispositivo electrónico u otro dispositivo en un servidor del proveedor de servicios.

10. Procedimiento según una de las reivindicaciones 1 a 8, en el que se realiza la comunicación entre el dispositivo electrónico y el servidor y sirve para transmitir información de autenticación desde el servidor al dispositivo electrónico, que es información de autenticación necesaria para un proceso de inicio de sesión y/o transacción que el usuario del dispositivo electrónico desea realizar con el dispositivo electrónico en un servidor de un proveedor de servicios.

11. Procedimiento realizado en un servidor (2) que está conectado comunicativamente a un dispositivo electrónico (3), comprendiendo el procedimiento:
- autenticar al usuario del dispositivo electrónico (3) y/o al dispositivo electrónico (3);

- proporcionar una primera clave para descifrar datos cifrados almacenados en dicho dispositivo electrónico (3) mediante un software almacenado en dicho dispositivo electrónico (3) y estando dichos datos descifrados destinados a una comunicación de dicho dispositivo electrónico (3), o bien
la primera clave junto con datos almacenados en el dispositivo electrónico (3) está destinada a una comunicación del dispositivo electrónico (3);
la primera clave se almacena de forma permanente sólo en el servidor (2),
caracterizado en que
el procedimiento comprende además en una fase de inicialización:
- comprobar por parte del servidor (2) al menos una característica del software almacenado en el dispositivo electrónico (3) y al menos una característica del dispositivo electrónico (3); y
- suministrar la primera clave al dispositivo electrónico (3), en el que dicho suministro sólo se produce después de una comprobación satisfactoria.

12. Procedimiento según la reivindicación 11, en el que la al menos una característica del software almacenado en el dispositivo electrónico (3) representa su integridad con respecto a un estado original o un estado derivable del mismo mediante actualizaciones oficiales.

13. Programa informático que comprende instrucciones de programa que hacen que un procesador ejecute y/o controle las etapas del procedimiento según una cualquiera de las reivindicaciones 1 a 10 u 11 y 12 cuando el programa informático se está ejecutando en el procesador.

14. Conjunto de desarrollo de programas informáticos que tiene unos bloques de construcción de programas informáticos que incluyen instrucciones de programa que hacen que un procesador ejecute las etapas del procedimiento según una cualquiera de las reivindicaciones 1 a 10 u 11 y 12 cuando un programa informático creado a partir de dichos bloques de construcción de programas informáticos se ejecuta en dicho procesador.

15. Dispositivo que comprende medios para realizar el procedimiento según una cualquiera de las reivindicaciones 1 a 10 u 11 y 12.

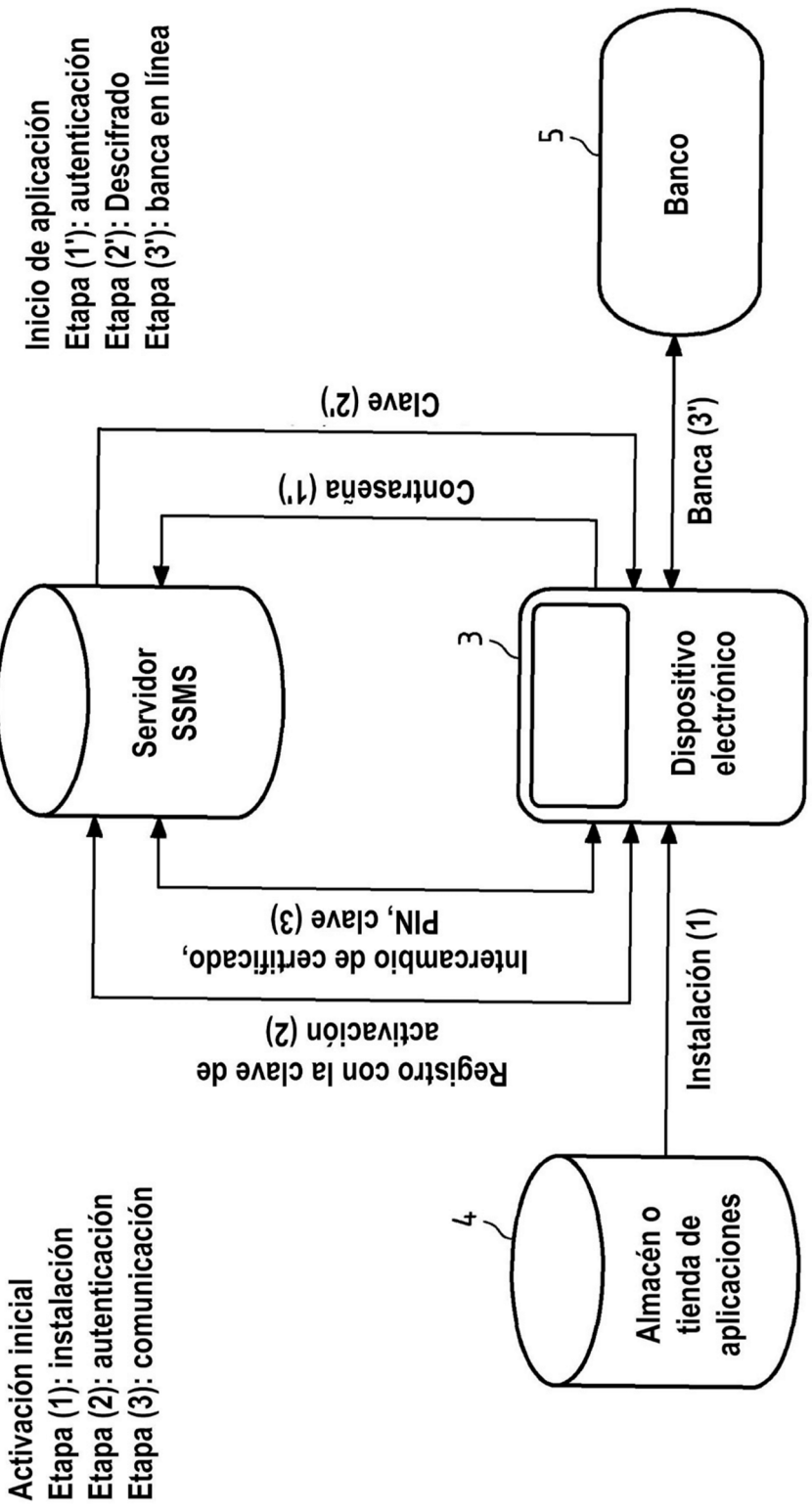
Inicio de aplicación
Etapa (1'): autenticación
Etapa (2'): Descifrado
Etapa (3'): banca en línea
1
Clave (2')
Contraseña (1')
Banca (3')
5
Banco
2
Servidor SSMS
3
Dispositivo electrónico
Intercambio de certificado, PIN, clave (3)
Registro con la clave de activación (2)
Instalación (1)
4
Almacén o tienda de aplicaciones
Activación inicial
Etapa (1): instalación
Etapa (2): autenticación
Etapa (3): comunicación

Fig.1

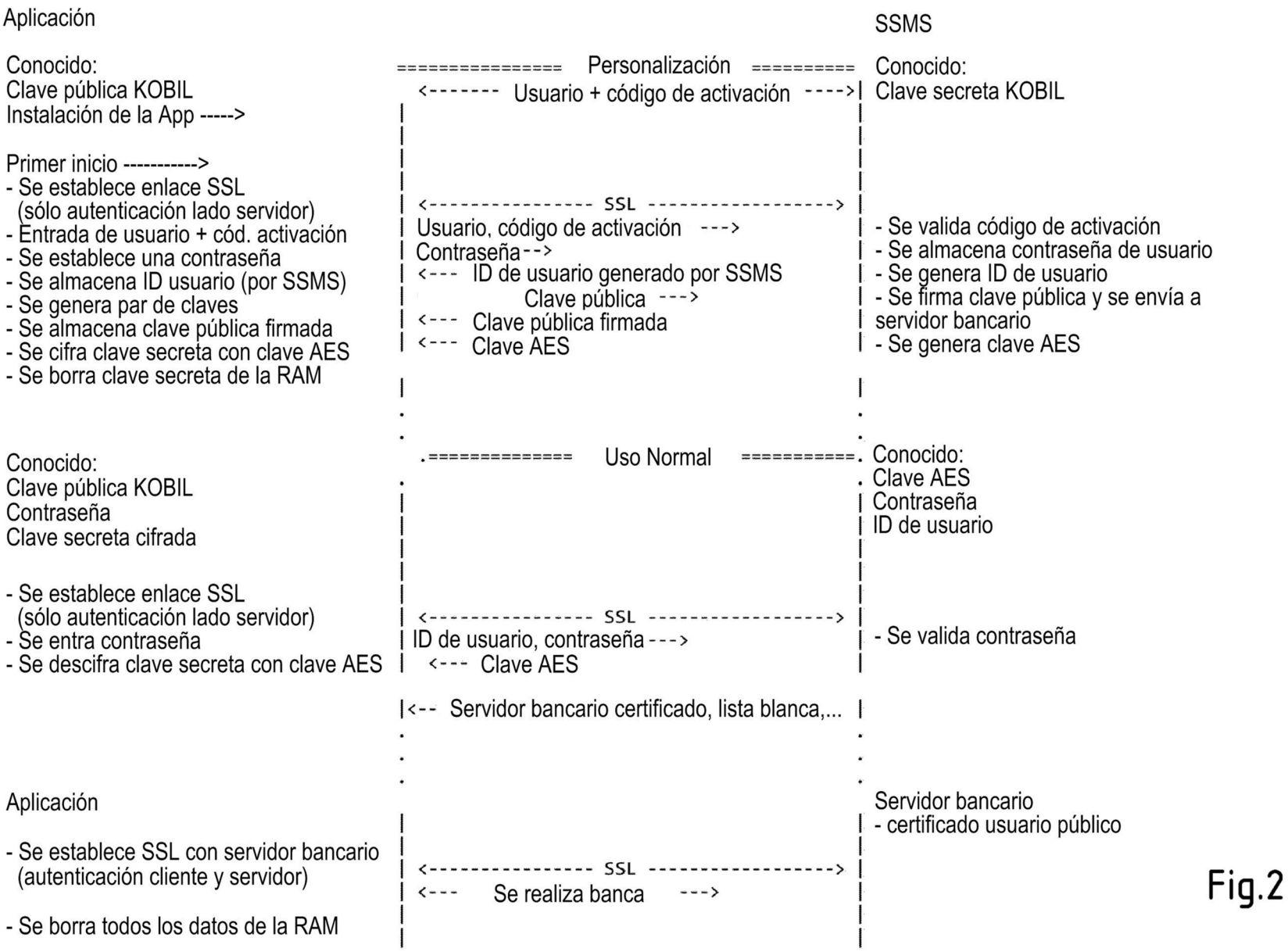

Fig.2

ES 2 739 896 T3

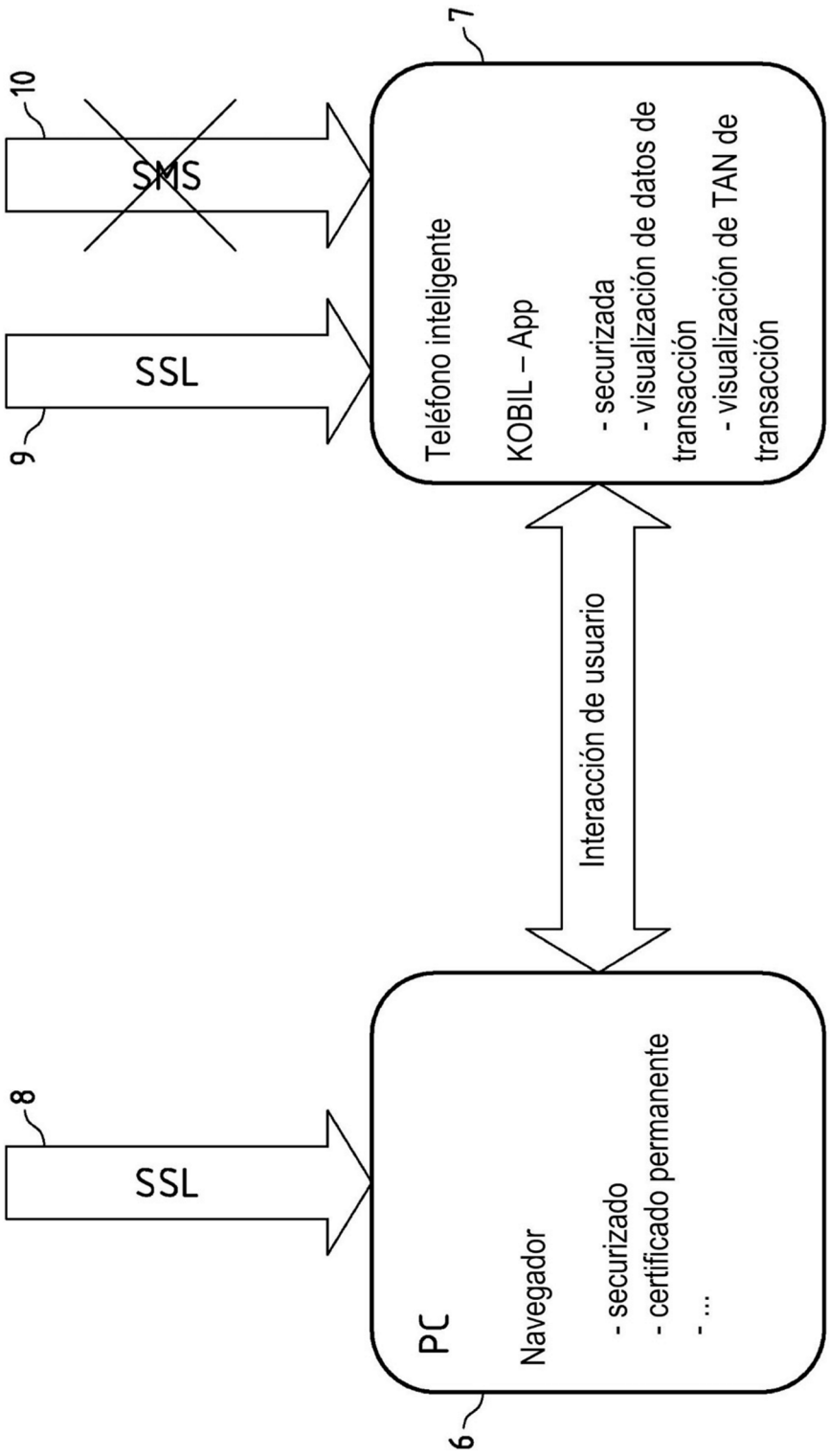
10
SMS
9
SSL
7
Teléfono inteligente
KOBIL – App
- securizada
- visualización de datos de transacción
- visualización de TAN de transacción
Interacción de usuario
8
SSL
6
PC
Navegador
- securizado
- certificado permanente
- ...

Fig.3

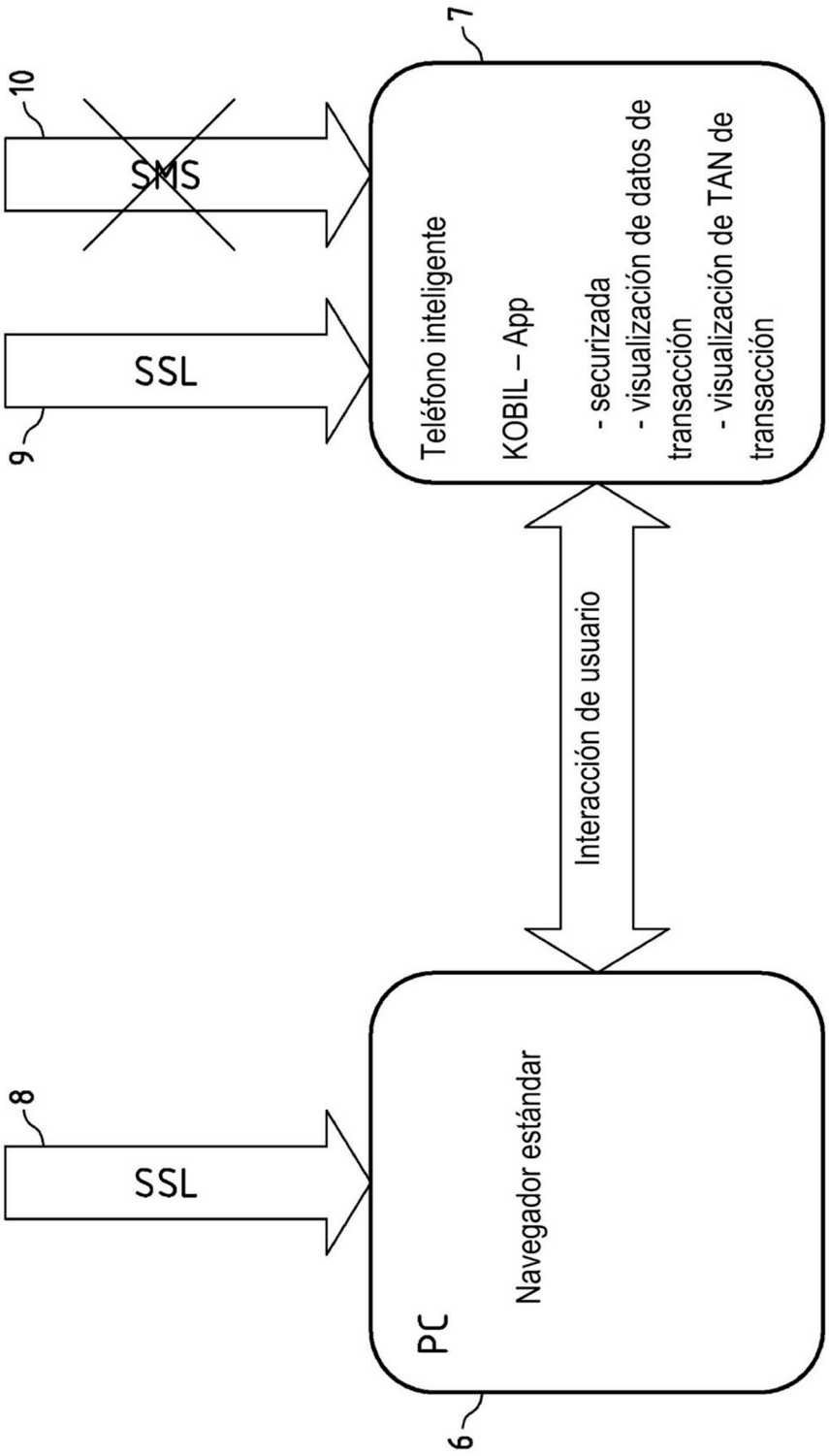
10
SMS
SSL
9
7
Teléfono inteligente
KOBIL – App
- securizada
- visualización de datos de transacción
- visualización de TAN de transacción
Interacción de usuario
8
SSL
PC
Navegador estándar
6

Fig.4a

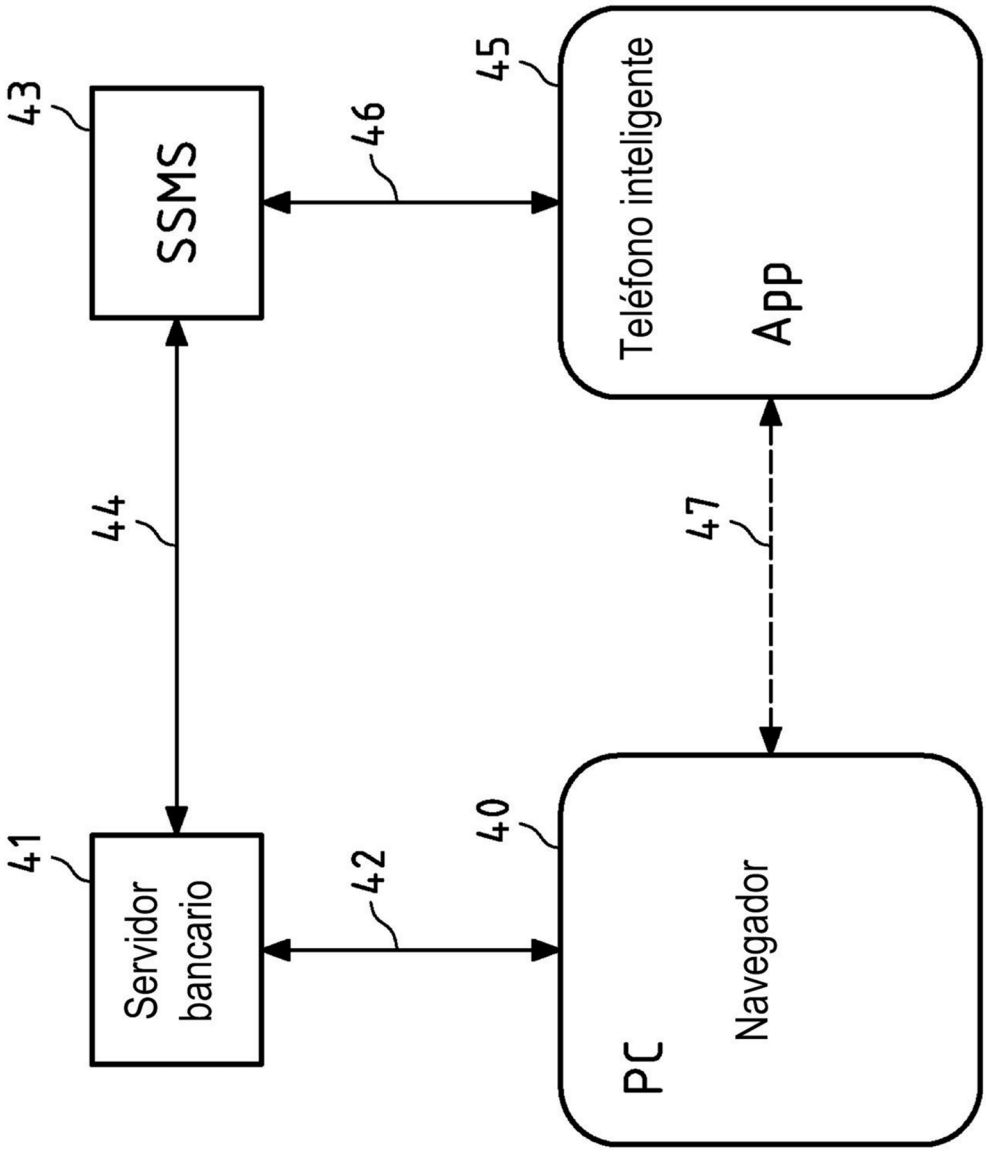
43
SSMS
46
45
Teléfono inteligente
App
44
47
41
Servidor bancario
42
40
PC
Navegador

Fig.4b

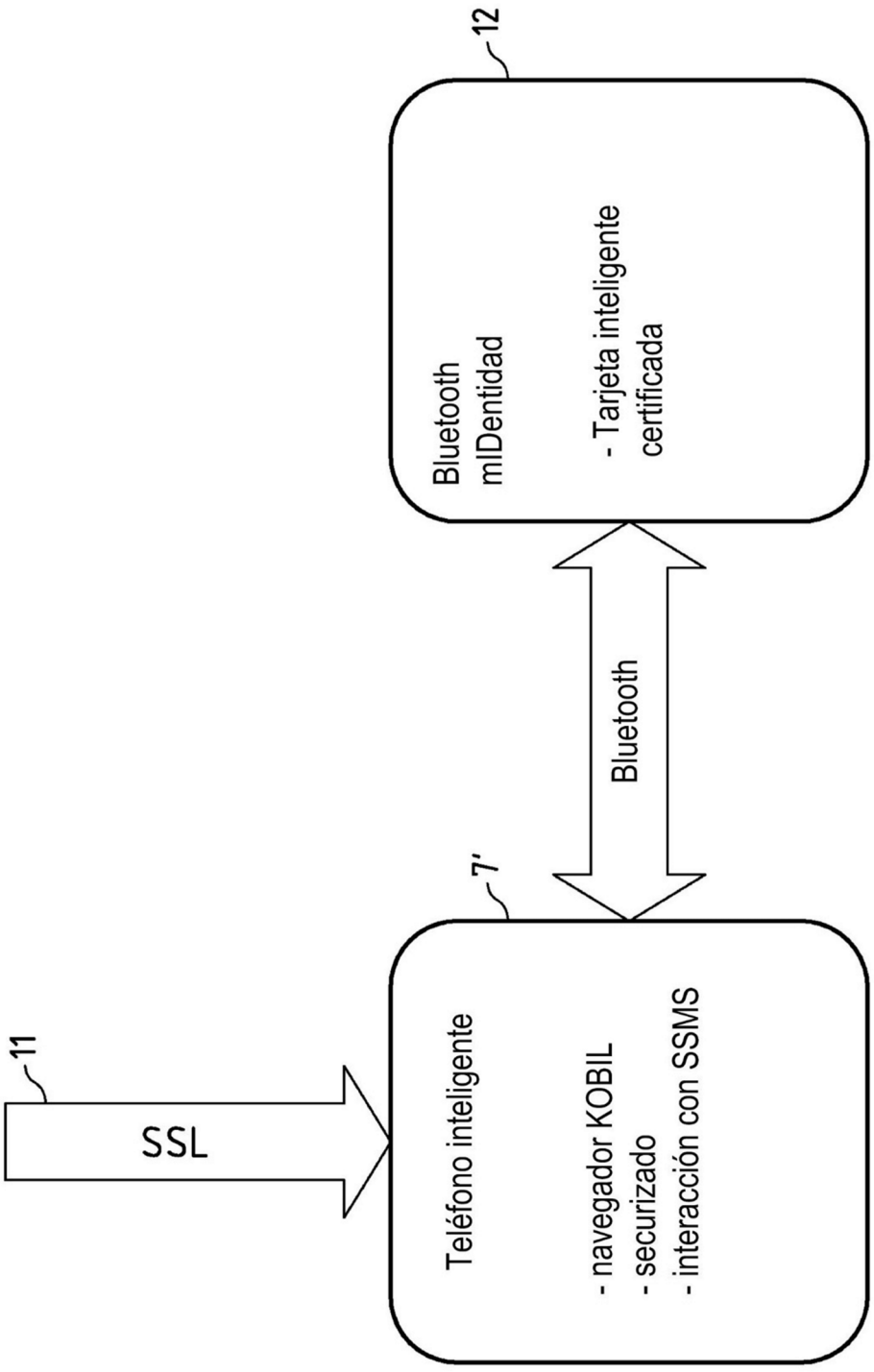
11
SSL
Teléfono inteligente
- navegador KOBIL
- securizado
- interacción con SSMS
7'
Bluetooth
12
Bluetooth
mIDentidad
- Tarjeta inteligente
certificada

Fig.5a

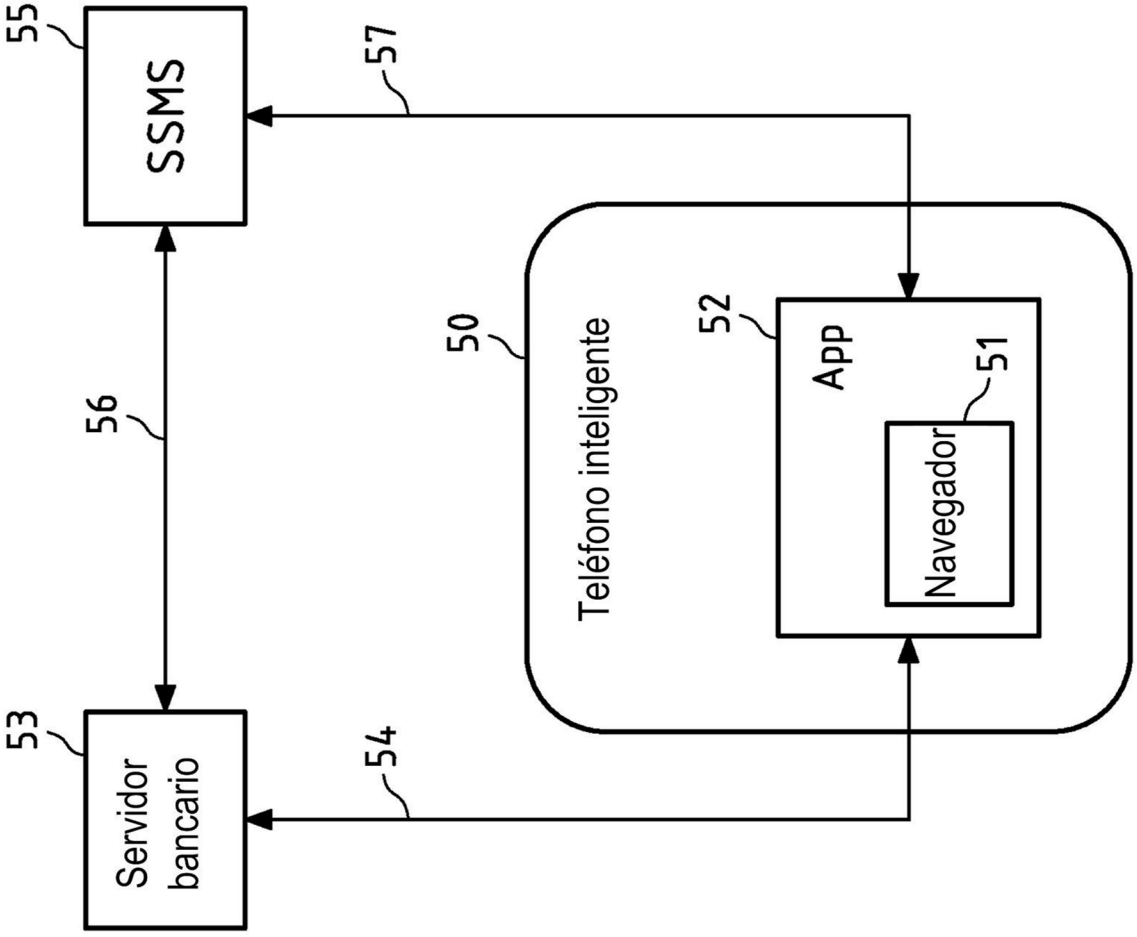
55
SSMS
57
56
50
Teléfono inteligente
52
App
51
Navegador
53
Servidor bancario
54

Fig.5b

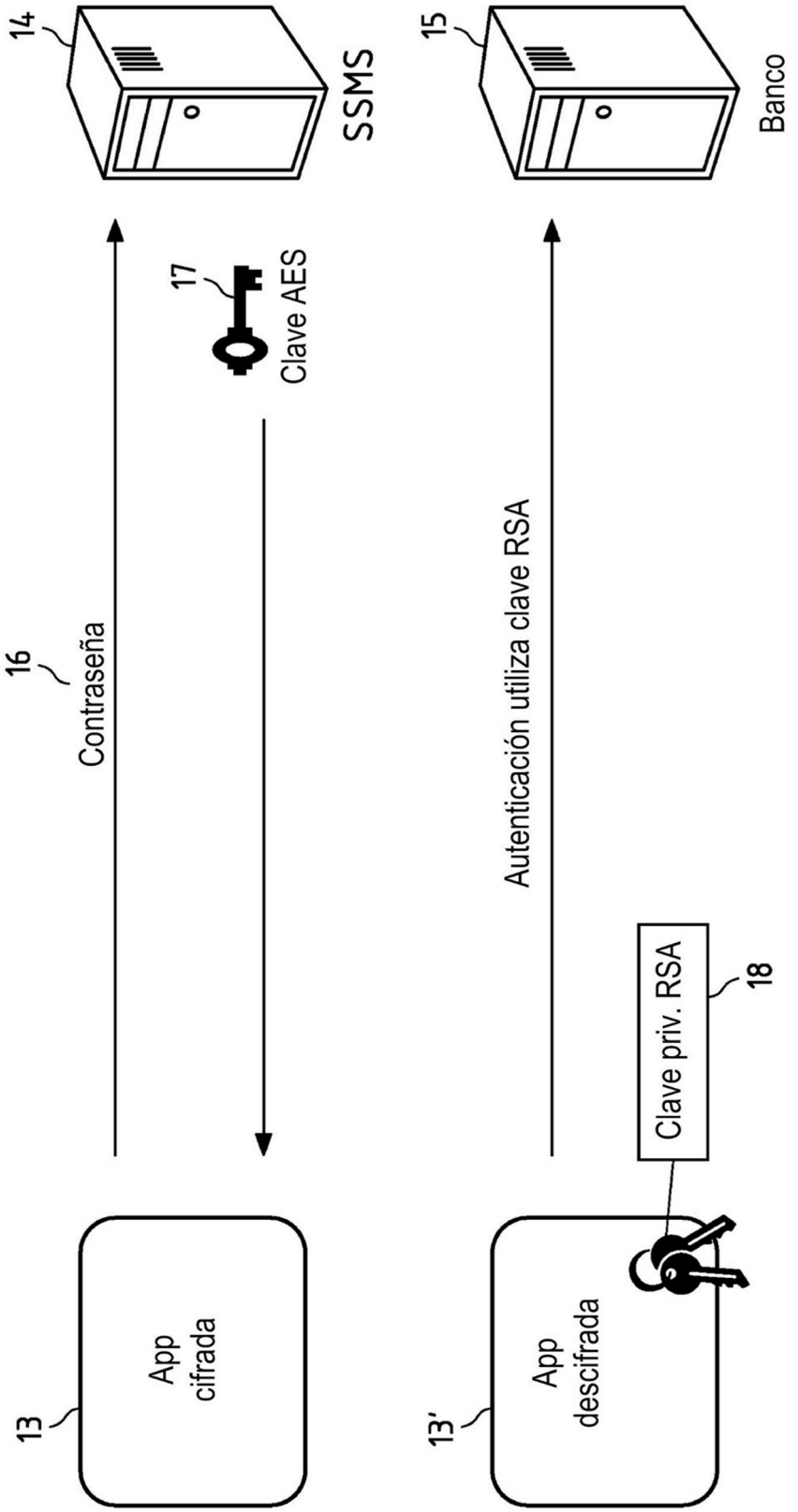
14
SSMS
15
Banco
17
Clave AES
16
Contraseña
Autenticación utiliza clave RSA
Clave priv. RSA
18
13
App cifrada
13'
App descifrada

Fig.6

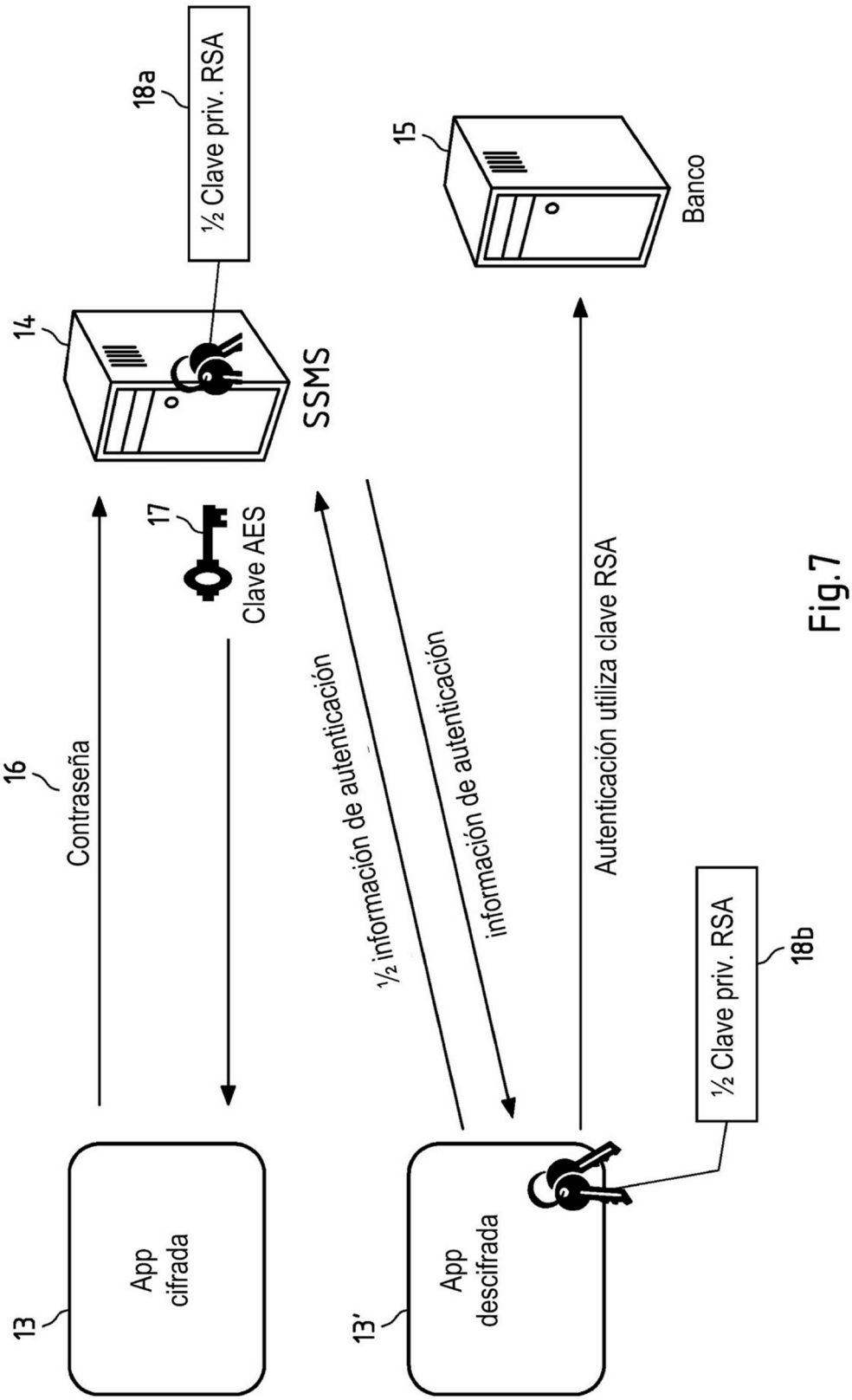
18a
½ Clave priv. RSA
14
SSMS
15
Banco
17
Clave AES
16
Contraseña
½ información de autenticación
información de autenticación
Autenticación utiliza clave RSA
13
App cifrada
13'
App descifrada
½ Clave priv. RSA
18b

Fig.7

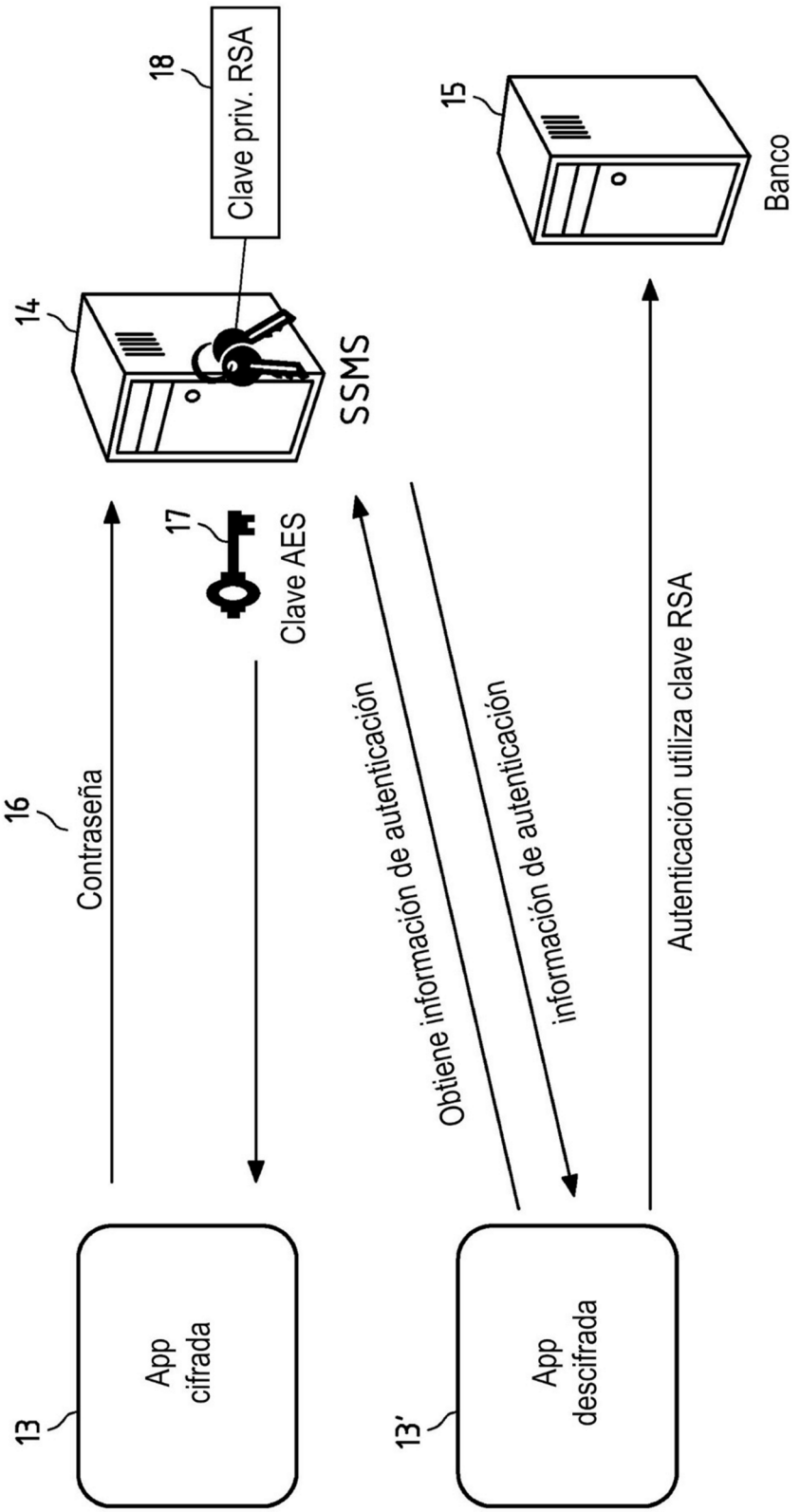
18
Clave priv. RSA
15
Banco
14
SSMS
17
Clave AES
16
Contraseña
Obtiene información de autenticación
información de autenticación
Autenticación utiliza clave RSA
13
App cifrada
13'
App descifrada

Fig.8

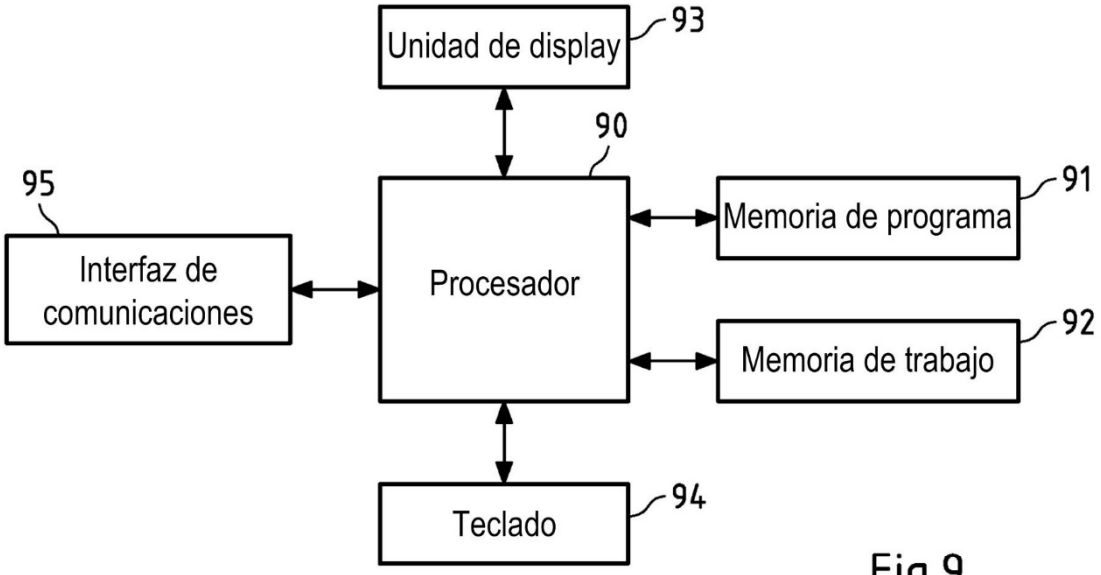

Fig.9

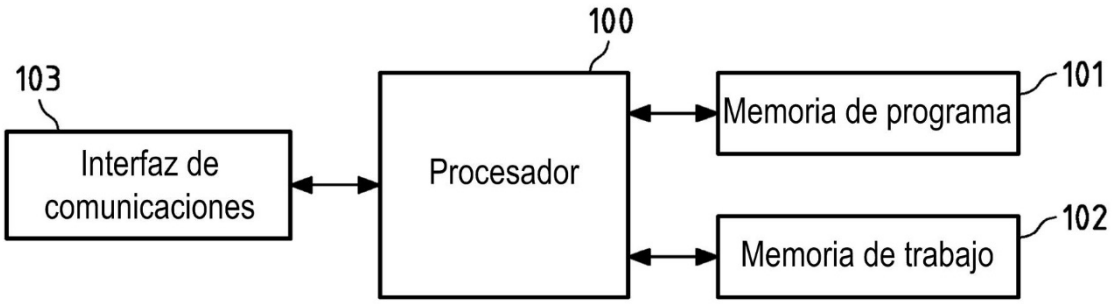

Fig.10

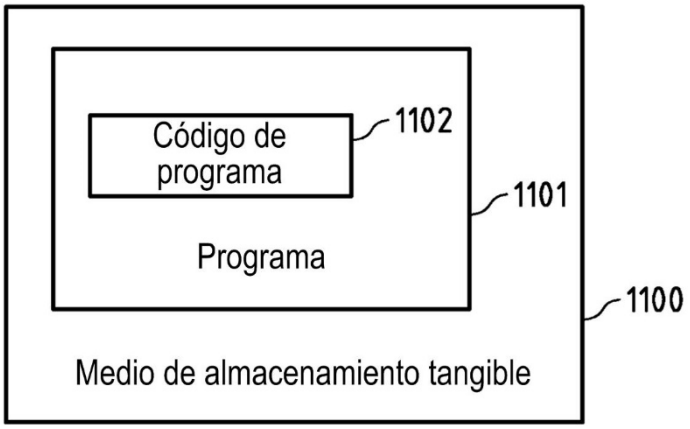

Fig.11