(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 500 947**

(51) Int. CI.:

***G06F 21/00*** (2013.01)
***H04L 9/32*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.09.2011 E 11182188 (0)**

(97) Fecha y número de publicación de la concesión europea: **11.06.2014 EP 2434424**

(54) Título: **Procedimiento para aumentar la seguridad de servicios en línea relevantes con respecto a la seguridad**

(30) Prioridad:

**27.09.2010 DE 102010037784**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**01.10.2014**

(73) Titular/es:

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

(72) Inventor/es:

**KOYUN, ISMET y**
**TAK, MARKUS**

(74) Agente/Representante:

**VEIGA SERRANO, Mikel**

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

Procedimiento para aumentar la seguridad de servicios en línea relevantes con respecto a la seguridad

**Sector de la técnica**

La invención se refiere a un procedimiento para aumentar la seguridad de servicios en línea relevantes con respecto a la seguridad. La invención se refiere además a un programa informático correspondiente, a un dispositivo de soporte de datos correspondiente, a un equipo de procesamiento de datos correspondiente, a un sistema correspondiente y a un paquete de datos correspondiente.

**Estado de la técnica**

Hoy en día se realizan un gran número de servicios relevantes con respecto a la seguridad a través de Internet. Así, por ejemplo, se conoce realizar operaciones bancarias o pagos a través de Internet. Sin embargo, las aplicaciones en línea, como la banca en línea o el pago en línea constituyen un blanco para los piratas informáticos, que pretenden averiguar los datos relevantes con respecto a la seguridad de un usuario y realizar en su nombre con estos datos transacciones en línea. Por ejemplo se sustraen los datos de autenticación del usuario por medio de diferentes técnicas, como las técnicas de suplantación de identidad (*phishing*) o troyanos, y a continuación se utilizan para el pago.

Según el estado de la técnica los servicios relevantes con respecto a la seguridad, como la banca en línea y similares, se realizan a través de programas de acceso a red, como por ejemplo los navegadores de Internet habituales y similares. A través de un programa de navegación de este tipo un usuario abre por ejemplo una página de Internet de un proveedor de servicios, por ejemplo de un banco. Sin embargo, antes de que el usuario pueda realizar una transacción relevante con respecto a la seguridad o un servicio como una transferencia, el usuario se autentica ante el banco. Para ello el usuario debe introducir por ejemplo el nombre de usuario y una contraseña. Por tanto, el usuario transmite desde su equipo de procesamiento de datos, como un ordenador, al menos una característica de autenticación al banco, en particular a su equipo de procesamiento de datos, como un servidor. Los datos transmitidos se comparan con datos almacenados por el banco y en caso de un resultado de comparación positivo se permite al usuario la realización del servicio correspondiente. Una autenticación también puede realizarse mediante otras operaciones criptográficas, como por ejemplo una verificación de firma.

Sin embargo, mediante las técnicas mencionadas anteriormente de los piratas informáticos, en particular mediante un ataque denominado “Man In The Browser”, es posible manipular un programa de acceso a red, como por ejemplo un navegador de Internet. Así, por ejemplo, en el caso de una manipulación de un navegador de Internet es posible que un usuario introduzca sus datos de autenticación, como por ejemplo un número PIN, una contraseña o similares de la manera habitual para activar el correspondiente servicio o la transacción, como una transferencia. Sin embargo, mediante la manipulación del navegador de Internet el dinero no se transfiere al destinatario deseado, sino a una cuenta indicada por el pirata informático.

Por el estado de la técnica, para mejorar la seguridad se conocen procedimientos en los que se utilizan componentes de hardware. Por ejemplo se utilizan procedimientos con contraseñas de un solo uso y tarjetas inteligentes. Estos procedimientos se denominan también procedimientos de autenticación de 2 factores (tenencia y conocimiento). Por un lado, un usuario “conoce” algo, por ejemplo, la contraseña, y por otro el usuario “tiene” algo, por ejemplo la tarjeta inteligente, un dispositivo de almacenamiento masivo USB, etc. Si bien esta autenticación de 2 factores aumenta la seguridad, sin embargo en este procedimiento también aumentan los costes. En particular en el caso de una gran difusión, que en el caso de la banca en línea puede ser del orden de millones, los costes son elevados.

Por la solicitud de patente WO 2008/034900 A1 se conoce un procedimiento para la protección de un programa informático frente a una manipulación y para proteger su comunicación con otros programas frente a interceptación. El procedimiento comprende generar copias de programa individualizadas para diferentes grupos de usuarios, la inserción o derivación de claves criptográficas individuales a partir del código de programa, la ocultación del código de programa y la autoautenticación del programa frente a otros programas. El procedimiento puede aplicarse para la protección de banca en línea, inversión en línea, entretenimiento en línea, gestión de derechos digitales y otras aplicaciones de comercio electrónico.

Por la solicitud de patente US 2001/051928 A1 se conoce una disposición, un procedimiento y un sistema para la personalización de software publicado según un usuario autorizado específico. A este respecto se posibilita una protección frente a una copia y distribución no autorizadas desalentando al usuario autorizado para que no cree y distribuya sin orden ni concierto copias no autorizadas. La personalización está insertada en los software y se suministra al usuario autorizado con información personalizada incrustada ya existente sin que el usuario tenga que introducir esta información durante una configuración o una instalación. Como la información ya está incrustada en el software publicado que puede entregarse cuando el usuario lo recibe, y no es necesaria una introducción manual por parte del usuario, puede aplicarse una criptografía considerable con claves complejas para la autenticación y con

fines de protección. Como cada entrega a un usuario autorizado se basa en una construcción de software individual, personalizada, los módulos ejecutables de cada una de las copias autorizadas distribuidas del software tienen una forma binaria unívoca que puede variar de manera significativa, incluyendo variaciones en el tamaño de los módulos ejecutables, mientras que la funcionalidad de usuario es completamente idéntica. Estas variaciones llevan a una protección adicional del software al eliminar direcciones de programa constantes, que pueden analizarse y atacarse fácilmente con programas automatizados que anulan la protección.

Por la solicitud de patente US 2008/0034210 A1 se conoce un sistema de comunicación de datos seguro y un procedimiento para su utilización junto con un ordenador principal posiblemente no seguro. El sistema presenta un medio de almacenamiento, que puede unirse con el ordenador posiblemente no seguro. El sistema presenta también un navegador protegido autónomo que está almacenado en el medio de almacenamiento. El sistema también puede presentar datos de autenticación de cliente y/o datos de programa adicionales. El navegador puede utilizar los datos de autenticación de cliente para posibilitar una comunicación segura. Los datos de autenticación de cliente pueden estar almacenados en el medio de almacenamiento. Una forma de realización de la solicitud de patente US 2008/0034210 A1 se refiere a un soporte de datos extraíble que posibilitará una autenticación de 2 factores.

Por la patente US 6.108.420 se conoce un procedimiento para generar una instancia única, especifica del usuario, de una aplicación de software, distribuirla e instalarla en un ordenador de instalación, en el que la instancia de la aplicación de software puede autenticarse y atribuirse a un usuario determinado. Un agente de distribución seguro que se encuentra en un ordenador de distribución, recoge información de identificación y calcula una firma criptográfica de la aplicación de software y de la información de identificación. La información de identificación y la firma criptográfica se incrustan mediante el agente de distribución seguro en la aplicación de software. La aplicación de software con los datos incrustados puede transmitirse mediante un canal de distribución al ordenador de instalación. Un agente de instalación de usuario, que se encuentra en el ordenador de instalación, controla la instalación de la aplicación de software con los datos incrustados en el ordenador de instalación. Antes de la instalación el agente de instalación de usuario puede utilizar la firma criptográfica para verificar la autenticidad de la aplicación de software y la información de identificación. Una forma de realización de la patente US 6.108.420 se refiere al cifrado de contenidos originales con una clave privada mediante el agente de distribución seguro y la transmisión de la clave pública correspondiente con un archivo de distribución compuesto, que contiene los contenidos originales cifrados, a través del canal de distribución al agente de instalación de usuario. El agente de instalación de usuario descifra a continuación el archivo de distribución compuesto con la clave pública.

Por la solicitud de patente EP 1 471 405 A1 se conoce un procedimiento y un equipo para la protección de información frente a un uso no autorizado. La información que obtiene un usuario está cifrada mediante un procedimiento de cifrado asimétrico que utiliza una clave de usuario, que recibe un distribuidor de la información. Antes de la utilización se descifra la información con ayuda de una clave privada del usuario. Para aumentar la protección, el descifrado puede realizarse directamente en la CPU del ordenador del usuario de tal manera que la información descifrada no exista fuera del procesador.

**Objeto de la invención**

Por tanto, un objetivo de la presente invención es superar las desventajas mencionadas anteriormente.

Este objetivo se soluciona mediante un procedimiento según la reivindicación 1. Por lo demás, el objetivo en el que se basa la invención se consigue mediante un programa informático según la reivindicación 13, un equipo de procesamiento de datos según la reivindicación 14 y un sistema según la reivindicación 15. Pueden deducirse configuraciones ventajosas de las reivindicaciones dependientes.

El procedimiento según la invención comprende generar un paquete de datos, que comprende al menos un programa de acceso a red protegido y al menos una característica de autenticación personalizada, en un primer equipo de procesamiento de datos, comprendiendo el paquete de datos la al menos una característica de autenticación personalizada junto al al menos un programa de acceso a red, cifrar el paquete de datos y proporcionar el paquete de datos para una transmisión a un equipo de procesamiento de datos adicional, pudiendo descifrarse el paquete de datos transmitido con una clave personalizada en el equipo de procesamiento de datos adicional, de tal manera que el programa de acceso a red pueda ejecutarse y puede autenticarse mediante la característica de autenticación personalizada.

Según la invención se genera una clave personalizada. Por tanto puede generarse una clave individual y unívoca, que sólo está asignada a un único usuario, concretamente al usuario mencionado anteriormente. El paquete de datos individual generado sólo puede descifrarse con la clave personalizada. Esta clave también puede estar prevista para el cifrado del paquete de datos en el primer equipo de procesamiento de datos. Se entiende que, junto a este cifrado simétrico, también puede preverse un cifrado asimétrico, es decir claves diferentes para el cifrado y el descifrado.

Un programa de acceso a red con una función de protección, es decir un programa de acceso a red protegido, es por ejemplo un navegador protegido. Por protección se entiende en la técnica informática, por ejemplo, utilizar sólo

software dedicado, que es necesario para el funcionamiento del sistema y cuya correcta ejecución desde el punto de vista de los aspectos de la seguridad puede garantizarse. Así, en un programa de acceso a red protegido pueden eliminarse todos los componentes de software y funciones que no son obligatoriamente necesarios para desempeñar la función prevista por el programa de acceso a red.

La función de protección puede encargarse, en particular, de que el programa de acceso a red esté protegido durante la ejecución en un equipo de procesamiento de datos.

Junto a este programa de acceso a red, el paquete de datos comprende al menos una característica de autenticación personalizada. Una característica de autenticación personalizada es, por ejemplo, una característica individual y unívoca que sólo está asignada a un único usuario, como por ejemplo una contraseña, certificados de software o similares. Una relación de la característica de autenticación con el programa de acceso a red conduce a un paquete de datos personalizado. En particular, este paquete de datos está asignado a un único usuario y es unívoco. Con la característica de autenticación puede verificarse, por ejemplo, en el primer equipo de procesamiento de datos si el programa de acceso a red o el usuario del programa de acceso a red está autorizado para la realización de un servicio de un proveedor en línea. Cuando el usuario está autorizado, el programa de acceso a red puede autenticarse.

El paquete de datos generado se cifra. En particular, éste puede cifrarse antes de la transmisión del paquete de datos.

Tras un cifrado del paquete de datos, el paquete de datos puede proporcionarse para una transmisión al usuario, en particular a un equipo de procesamiento de datos adicional del usuario. Se entiende que el cifrado puede realizarse en el marco de la composición del paquete de datos. En particular, el paquete de datos se proporciona de manera que el usuario, conociendo la clave personalizada asignada al mismo, puede descifrar el paquete de datos en el equipo de procesamiento de datos adicional y ejecutar el programa de acceso a red y, tras una autenticación satisfactoria, realizar un servicio relevante con respecto a la seguridad. La clave personalizada es preferiblemente una clave individual y unívoca, que sólo está asignada a un único usuario. Puede utilizarse un procedimiento de cifrado simétrico o asimétrico.

Por ejemplo, el paquete de datos puede estar cifrado de manera simétrica con la clave personalizada. Es concebible que la clave personalizada corresponda a la característica de autenticación. No obstante, en este caso el usuario tendría conocimiento de la característica de autenticación.

También es concebible que la clave personalizada no corresponda a la característica de autenticación, de modo que el usuario no tenga conocimiento alguno de la característica de autenticación. Esto es ventajoso, por ejemplo, para evitar que el usuario emplee la característica de autenticación independientemente del programa de acceso a red.

Mediante el cifrado del paquete de datos generado puede producirse una asociación entre el programa de acceso a red y la característica de autenticación, por ejemplo de tal manera que la característica de autenticación sólo pueda utilizarse conjuntamente con el programa de acceso a red. La característica de autenticación y el programa de acceso a red están protegidos en el paquete de datos mediante el cifrado. La función de protección puede proteger el programa de acceso a red descifrado durante la ejecución del programa de acceso a red en una instalación de procesamiento de datos y/o la característica de autenticación descifrada.

A diferencia del estado de la técnica, se pone a disposición del usuario por tanto un programa especial para la realización de un servicio relevante con respecto a la seguridad, que está concebido exclusivamente para este servicio. Este programa está asociado ya con al menos una característica de autenticación. De este modo se reduce significativamente el riesgo de manipulaciones. En particular se fuerza a un usuario a utilizar el programa de acceso a red asignado al mismo y ningún otro. La característica de autenticación personalizada sólo está integrada en este paquete de datos y no en otros paquetes de datos. Además, para aumentar la seguridad, este programa se cifra antes de una transmisión de manera personalizada, es decir individual. En particular, el cifrado también puede servir para asociar la característica de autenticación de manera fija al programa de acceso a red. El usuario no puede separar por tanto ambos componentes y utilizar, por ejemplo, la característica de autenticación en otro programa de acceso a red. Además puede garantizarse una elevada seguridad, a diferencia de en el estado de la técnica, sin hardware adicional. Por consiguiente, con el procedimiento según la invención pueden reducirse los costes.

El programa informático según la invención comprende instrucciones de programa que permiten que un procesador realice el procedimiento según la invención, cuando el programa informático se ejecuta en el procesador. A este respecto el procesador puede formar parte por ejemplo del equipo de procesamiento de datos, en el que se realiza el procedimiento correspondiente. Un programa informático puede ser al menos parcialmente software y/o *firmware* de un procesador.

Un programa informático según la invención puede estar contenido por ejemplo en un dispositivo de soporte de datos, por ejemplo un medio de almacenamiento legible por ordenador, que por ejemplo está configurado como medio de almacenamiento magnético, eléctrico, electromagnético, óptico y/o de otro tipo.

Un dispositivo de soporte de datos de este tipo es por ejemplo portátil o puede estar instalado de manera fija en un dispositivo. Ejemplos de un dispositivo de soporte de datos de este tipo son memorias no volátiles con acceso aleatorio (RAM) como por ejemplo memorias flash NOR o con acceso secuencial como memorias flash NAND y/o memorias con acceso de sólo lectura (ROM) o acceso de escritura-lectura. Legible por ordenador se entenderá en particular como que el medio de almacenamiento puede leerse y/o describirse por un ordenador o un equipo de procesamiento de datos, por ejemplo por un procesador.

Un equipo de procesamiento de datos según la invención comprende medios para la realización del procedimiento según la invención, estando configurado el equipo de procesamiento de datos en relación con el software para poder realizar el procedimiento.

A este respecto, por configurado en relación con el software se entenderá en particular la preparación del equipo de procesamiento de datos que es necesaria para poder realizar un procedimiento por ejemplo en forma de un programa informático. Esta preparación se denomina a menudo instalación.

Es concebible que los programas informáticos según la invención se ejecuten con medios del equipo de procesamiento de datos según la invención, por ejemplo un procesador. Por procesador se entenderán, entre otros, unidades de control, microprocesadores, microunidades de control, como microcontroladores, procesadores digitales de señales (DSP), circuitos integrados de aplicación específica (ASIC) o disposiciones de puertas programables en campo (FPGA).

El equipo de procesamiento de datos según la invención comprende por lo demás medios para la unión con el dispositivo de soporte de datos. Estos medios pueden ser por ejemplo una interfaz de datos correspondiente a la interfaz de datos del dispositivo de soporte de datos.

El equipo de procesamiento de datos según la invención comprende un generador de autenticación para generar una característica de autenticación personalizada, un generador de paquete de datos para generar un paquete de datos que comprende al menos un programa de acceso a red con una función de protección y la característica de autenticación personalizada generada, un generador de clave para generar una clave personalizada, un generador de cifrado para cifrar el paquete de datos con la clave personalizada generada, y un módulo de transmisión para proporcionar el paquete de datos cifrado para una transmisión a un equipo de procesamiento de datos adicional, de modo que el paquete de datos transmitido puede descifrarse con la clave personalizada en el equipo de procesamiento de datos adicional, de tal manera que puede ejecutarse el programa de acceso a red.

El sistema según la invención comprende un equipo de procesamiento de datos según la invención y al menos un equipo de procesamiento de datos adicional. Por ejemplo, el equipo de procesamiento de datos según la invención puede ser un servidor, que se pone a disposición por un proveedor de servicios, mientras que los equipos de procesamiento de datos adicionales de los usuarios, que quieren hacer uso del servicio ofrecido, pueden ser por ejemplo ordenadores, teléfonos inteligentes y similares.

A continuación se describen configuraciones a modo de ejemplo de la presente invención, que se refieren a características adicionales a modo de ejemplo del procedimiento, programa informático, equipo de procesamiento de datos y sistema según la invención. En particular mediante la descripción de una etapa de procedimiento adicional del procedimiento según la invención también se darán a conocer medios para la realización de la etapa de procedimiento del equipo de procesamiento de datos según la invención correspondiente y una instrucción de programa correspondiente del programa informático según la invención correspondiente que permite que un procesador realice la etapa de procedimiento cuando el programa informático se ejecuta mediante el procesador. Lo mismo se aplica también para dar a conocer un medio para la realización de una etapa de procedimiento o una instrucción de programa, por ejemplo al dar a conocer un medio para la realización de una etapa de procedimiento también se dará a conocer la etapa de procedimiento correspondiente y una instrucción de programa correspondiente.

Según un ejemplo de realización adicional el procedimiento según la invención comprende además que el paquete de datos puede comprimirse en el primer equipo de procesamiento de datos. Dicho de otro modo puede reducirse el tamaño del paquete de datos para una transmisión más sencilla y rápida. El paquete de datos puede comprimirse, es decir, empaquetarse, en principio en cualquier fase antes de una transmisión. Sin embargo, preferiblemente la unión, el cifrado y la compresión de los componentes del paquete de datos pueden realizarse en una etapa de procedimiento dedicada.

Además en principio es posible insertar componentes adicionales en el paquete de datos. Según un ejemplo de realización adicional el paquete de datos puede comprender adicionalmente al menos un archivo de configuración, pudiendo establecer el archivo de configuración la configuración del programa de acceso a red al ejecutar el programa de acceso a red. Por ejemplo mediante la configuración, la apertura de una página de Internet del proveedor de servicios puede producirse automáticamente al iniciar un programa de acceso a red configurado como

navegador web. Igualmente dentro de este archivo de configuración pueden encontrarse ajustes para verificar la autenticidad de la página de Internet solicitada.

Para evitar que no sean visibles archivos no cifrados como resultado intermedio durante la etapa de descifrado y dado el caso de descompresión, según un ejemplo de realización de la invención el procedimiento según la invención puede comprender además que el paquete de datos pueda descifrarse en una memoria volátil del equipo de procesamiento de datos adicional. En el caso de la memoria volátil puede tratarse de una memoria de trabajo, como una memoria RAM. Se entiende que también puede realizarse una eventual descompresión del paquete de datos en la memoria de trabajo.

Para que también durante la ejecución del programa de acceso a red no se hagan visibles resultados intermedios, alternativa o adicionalmente a un descifrado en una memoria de trabajo según un ejemplo de realización adicional puede estar previsto que la ejecución del programa de acceso a red pueda realizarse directamente (y por ejemplo exclusivamente) desde la memoria volátil del equipo de procesamiento de datos adicional. Entonces, por ejemplo, puede no ser necesaria una instalación del navegador. De este modo puede dificultarse adicionalmente un ataque potencial.

Por ejemplo, el programa de acceso a red y/o la característica de autenticación puede descifrarse directamente en una zona de una memoria de trabajo de la instalación de procesamiento de datos adicional y ejecutarse desde la memoria de trabajo de tal manera que el programa de acceso a red descifrado, la característica de autenticación descifrada y/o los resultados intermedios durante la ejecución del programa de acceso a red sólo estén almacenados en la memoria de trabajo.

Tras finalizar el programa de acceso a red puede liberarse por ejemplo la zona de la memoria de trabajo y sobrescribirse por otras aplicaciones. Alternativamente, la zona de la memoria de trabajo al finalizar el programa de acceso a red puede sobrescribirse con valores nulos o con valores aleatorios, para borrar de manera segura información residual en la memoria de trabajo, en particular la característica de autenticación descifrada. En caso contrario, otra aplicación, que a continuación acceda a la misma zona de la memoria de trabajo, podría obtener esta información. También es concebible que la zona de la memoria de trabajo se cifre antes de la liberación para garantizar una seguridad especialmente elevada. No obstante, la liberación también puede producirse sin un cifrado de la zona de la memoria de trabajo. La memoria de trabajo es preferiblemente una memoria de trabajo física, por ejemplo una memoria volátil, por ejemplo una memoria con acceso aleatorio. La memoria de trabajo puede ser una memoria principal, por ejemplo una memoria caché.

En este ejemplo no tiene lugar un almacenamiento (intermedio) del programa de acceso a red descifrado, de la característica de autenticación descifrada y/o de los resultados intermedios en una memoria de programa como un disco duro. De este modo al menos se dificulta el espionaje del programa de acceso a red descifrado, de la característica de autenticación descifrada y/o de los resultados intermedios durante la ejecución del programa de acceso a red en la instalación de procesamiento de datos adicional.

Para mejorar adicionalmente la seguridad, según un ejemplo de realización adicional según la invención puede estar previsto que al ejecutar el programa de acceso a red pueda supervisarse el estado del programa de acceso a red ejecutado. Por ejemplo, la función de protección del programa de acceso a red puede estar configurada de tal manera que durante todo el tiempo de ejecución del programa de acceso a red pueda supervisarse su estado. Así, en particular, puede supervisarse si otro proceso intenta engancharse en el espacio de proceso del programa de acceso a red, por ejemplo mediante depuradores (*Debugger*), hilos remotos (*Remote Threads*) o enlace (*Hooking*), para manipular su comportamiento, desactivar la función de protección o leer la característica de autenticación individual del usuario o la clave personalizada. Además en caso de detectar un ataque pueden aplicarse contramedidas adecuadas y mostrarse al menos el ataque al usuario y/o al proveedor de servicios así como interrumpirse la transacción. Puede bloquearse un acceso adicional por medio del programa de acceso a red individual y puede ser necesaria una generación y transmisión de un nuevo paquete de datos.

Alternativa o adicionalmente, la protección del programa de acceso a red puede comprender por ejemplo también el uso de denominados métodos de ofuscación de código. Por ejemplo se oculta el código fuente del programa de acceso a red de tal manera que durante el tiempo de ejecución del programa de acceso a red se evita una deducción de la estructura del programa y/o los estados internos del programa de acceso a red como resultados intermedios. En particular los métodos de ofuscación de código son adecuados para evitar una denominada ingeniería inversa del programa de acceso a red (por ejemplo durante el tiempo de ejecución).

Por lo demás, según otro ejemplo de realización de la invención está previsto que el paquete de datos y la clave personalizada correspondiente se transmitan por separado. Una transmisión por separado de estos componentes se garantiza al menos cuando los componentes se transmiten por diferentes trayectos de comunicación y/o diferentes tiempos. Según un ejemplo de realización según la invención, la clave personalizada puede transmitirse por SMS, correo electrónico, certificado o servicio de mensajería y el paquete de datos puede transmitirse mediante descarga o como soporte de datos (por ejemplo CD-ROM o lápiz USB). El soporte de datos puede transmitirse por ejemplo también por correo. En este caso, entonces, la clave puede transmitirse al menos en otro bulto postal,

preferiblemente con retardo en el tiempo y en particular a través de otra vía de comunicación. De este modo se dificulta adicionalmente el espionaje de los datos relevantes con respecto a la seguridad.

Además se ha reconocido que la seguridad puede aumentarse adicionalmente en particular cuando un gran número de usuarios quieren utilizar un servicio ofrecido, cuando según un ejemplo de realización adicional el programa de acceso a red se modifica al menos parcialmente de manera personalizada. Por ejemplo la función de protección del programa de acceso a red puede modificar de manera personalizada partes especialmente sensibles con respecto a la seguridad del programa de acceso a red. En el caso de un ataque satisfactorio, un atacante sólo puede anular un único programa de acceso a red, no sin embargo los programas de acceso a red modificados individualmente de los demás usuarios. Puede evitarse una transmisión del ataque a otros usuarios y por tanto un aprovechamiento masivo del ataque.

Para posibilitar una autenticación en un proveedor de servicios, según un ejemplo de realización adicional de la invención puede estar previsto que la característica de autenticación personalizada del paquete de datos y la clave personalizada correspondiente al paquete de datos puedan asignarse a un usuario, y que esta asignación pueda almacenarse en una base de datos del primer equipo de procesamiento de datos. Como base de datos puede utilizarse en principio cualquier medio de almacenamiento adecuado. También se entiende que la base de datos no tiene que disponerse en el propio equipo de procesamiento de datos, sino que sólo es necesario que el equipo de procesamiento de datos pueda acceder a la base de datos. Así, por ejemplo, el primer equipo de procesamiento de datos puede estar configurado como servidor proveedor de servicios y la base de datos como servidor de base de datos.

Para una autenticación, según un ejemplo de realización adicional de la invención, la autenticación del usuario del equipo de procesamiento de datos adicional con respecto al primer equipo de procesamiento de datos por medio de la característica de autenticación personalizada puede realizarse de tal manera que el usuario pueda realizar un servicio relevante con respecto a la seguridad exclusivamente en caso de autenticación positiva. En caso de que falle la autenticación, por ejemplo porque en la base de datos no está depositada ninguna característica de autenticación correspondiente para este usuario, puede prohibirse una realización del servicio relevante con respecto a la seguridad.

El procedimiento según la invención, el equipo de procesamiento de datos según la invención y el sistema según la invención pueden utilizarse preferiblemente en aplicaciones en línea relevantes con respecto a la seguridad, como por ejemplo en la banca en línea o en el pago en línea. Estas aplicaciones pueden utilizarse por un gran número de usuarios, obteniendo cada usuario un paquete de datos adaptado en cada caso individualmente al usuario, es decir, unívoco.

Ejemplos de realización de la presente invención se refieren entre otros a la problemática descrita a continuación. La seguridad en aplicaciones web críticas con respecto a la seguridad puede aumentarse porque se utilizan denominados testigos de seguridad. Tales testigos tienen dos propiedades importantes:

S1 Protegen aplicaciones críticas con respecto a la seguridad (banca en línea, pago en línea, etc.) frente a un abuso por usuarios no autorizados. Contienen como característica de autenticación secreta una clave secreta. Este secreto puede utilizarse para autenticar el propietario del testigo en relación con una aplicación crítica con respecto a la seguridad. Este secreto está protegido porque está depositado en una zona inaccesible del testigo.

S2 Protegen a los usuarios de aplicaciones críticas con respecto a la seguridad frente a ataques de piratas informáticos. Contienen un navegador protegido que evita que un atacante pueda manipular el navegador.

Los ejemplos de realización de la invención se basan entre otros en el reconocimiento de que puede alcanzarse la misma protección mediante una solución de software pura proporcionando el proveedor del servicio crítico con respecto a la seguridad a cada usuario por ejemplo un software individual que asuma las funciones de seguridad anteriores. Este software tiene las siguientes propiedades:

E1 Comprende o está compuesto por un navegador que está unido de manera fija con una característica de autenticación. Esta característica de autenticación preferiblemente ni es legible ni puede modificarse.

E2 El navegador está protegido y está individualizado para cada usuario.

La propiedad E1 garantiza por ejemplo la propiedad de seguridad S1. La propiedad E2 garantiza por ejemplo la propiedad de seguridad S2. La protección reduce el navegador a lo esencial y así reduce las posibilidades de ataque. La protección complementa funciones de seguridad adicionales que evitan ataques conocidos como inyección de código. La individualización evita que sean posibles ataques frente a un gran número de usuarios, porque concretamente los ataques también tienen que individualizarse.

La propiedad E1 se alcanza por ejemplo porque antes de la entrega del software éste se une con la característica de autenticación y se cifra el software así producido individualmente para cada usuario. La propiedad E2 se alcanza por ejemplo porque se llevan a cabo las medidas de protección habituales y se realiza una individualización de código. La seguridad puede favorecerse mediante medidas adicionales. El navegador protegido puede descifrarse individualmente por ejemplo para cada aplicación, concretamente en la memoria principal del ordenador de cliente.

La protección de la característica de autenticación puede proporcionarse por un lado mediante el código de activación o la contraseña del usuario, que ha obtenido en un canal separado, y por otro lado también mediante los diferentes mecanismos de protección, que evitarán un ataque de la memoria del proceso del navegador en el momento de ejecución. La ofuscación de código y los demás mecanismos de protección se encargan por ejemplo de que el proceso del navegador se proteja en el momento de ejecución (es decir, por ejemplo en la memoria, por ejemplo la memoria de trabajo). El cifrado de todo el paquete de datos, es decir del navegador y de la característica de autenticación se encarga por ejemplo de que el navegador también esté protegido en el disco duro (por ejemplo frente a un robo) y que el atacante no pueda hacer nada (todavía necesita el código de activación).

Por ejemplo, así, la característica de autenticación casi siempre está solamente cifrada y sólo se descifra en el momento de ejecución y esto sólo en la memoria de trabajo, concretamente en un navegador protegido. De este modo se reduce considerablemente la posibilidad de sustraer la característica de autenticación.

Las configuraciones a modo de ejemplo de la presente invención descritas en esta memoria descriptiva también se dan a conocer en cualquier combinación entre sí.

A partir de la siguiente descripción detallada de algunas formas de realización a modo de ejemplo de la presente invención, en particular en relación con las figuras, se deducirán configuraciones a modo de ejemplo de la invención adicionales ventajosas.

Sin embargo, las figuras adjuntas a la solicitud sólo servirán para aclarar, no sin embargo para determinar el alcance de protección de la invención. Los dibujos adjuntos no son a escala y sólo representarán el concepto general de la presente invención a modo de ejemplo. En particular las características, que están contenidas en las figuras, no deberán considerarse de ningún modo como componente necesario de la presente invención.

**Descripción de las figuras**

En las figuras, muestran

la figura 1 un primer diagrama de flujo con etapas de procedimiento de una forma de realización a modo de ejemplo de la invención;

la figura 2 un diagrama de bloques de una forma de realización a modo de ejemplo de un sistema con una forma de realización a modo de ejemplo de un equipo de procesamiento de datos; y

la figura 3 un segundo diagrama de flujo con etapas de procedimiento de una forma de realización a modo de ejemplo de la invención.

**Descripción detallada de la invención**

La figura 1 muestra un primer diagrama de flujo con etapas de procedimiento de una forma de realización a modo de ejemplo de la invención.

En una primera etapa (102) se genera un paquete de datos en un primer equipo de procesamiento de datos. El primer equipo de procesamiento de datos puede ser un ordenador, en particular un componente de servidor.

El paquete de datos, que se genera en la primera etapa (102), comprende al menos un programa de acceso a red protegido y una característica de autenticación personalizada. Un programa de acceso a red protegido es en particular un navegador web, que comprende una función de protección. También son concebibles otros programas de acceso a red, como un programa de banca en línea, en particular un programa de cliente, con función de protección.

Sin embargo, en el presente ejemplo de realización se parte de un navegador web protegido. Este navegador web comprende exclusivamente funciones, que son necesarias para la realización de los servicios relevantes con respecto a la seguridad deseados. De este modo puede reducirse claramente el riesgo de una manipulación del navegador web. En particular no pueden esconderse ataques por otros procesos, que se ejecutan continuamente en segundo plano en los navegadores habituales, de modo que se reconoce más fácilmente un ataque y pueden aplicarse contramedidas correspondientes. Además la función de protección puede comprender mecanismos contra ingeniería de inversión, contra depuración y contra inyección de código.

El navegador web se enlaza con una característica de autenticación personalizada, es decir, una característica individual y unívoca, que sólo está asignada a un único usuario. En particular, la característica de autenticación personalizada puede unirse de manera fija con el programa de acceso a red. De este modo se genera un paquete de datos individual para cada usuario.

Adicionalmente, el navegador web puede estar configurado de tal manera que estén modificados de manera personalizada partes del navegador web especialmente sensibles con respecto a la seguridad o se modifiquen individualmente por el propio navegador web mediante la función de protección. Esta medida aumenta en particular la seguridad de navegadores web adicionales de otros usuarios. Un atacante puede anular sólo una única instancia incluso en el caso de un ataque satisfactorio, pero de ningún modo las instancias de otros usuarios. Puede excluirse una transmisión del ataque a otros usuarios y por tanto un aprovechamiento masivo del ataque.

Una característica de autenticación, en particular en forma de software, puede ser por ejemplo una contraseña, certificados de software, como normas de criptografía de clave pública (PKCS), OpenSSL y similares. Se entiende que también pueden utilizarse varias características de autenticación en combinación para aumentar la seguridad.

En una siguiente etapa (104) de procedimiento se cifra el paquete de datos generado. El cifrado se produce con una clave personalizada, es decir una clave individual y unívoca, que sólo está asignada a un único usuario. Se conocen métodos de cifrado adecuados tales como ofuscación de código, cifrados criptográficos, por ejemplo *Advanced Encryption Standard* (AES) y similares. Por ejemplo en el caso de un cifrado simétrico con AES puede ponerse a disposición de un usuario la clave en un canal separado para “desempaquetar” el paquete de datos, de modo que también sólo éste pueda utilizarlo.

Tras el cifrado el paquete de datos puede transmitirse a un equipo de procesamiento de datos adicional, como un ordenador, portátil, teléfono inteligente y similares (etapa (106)). También es posible poner a disposición del usuario del equipo de procesamiento de datos el paquete de datos en un soporte de datos. Al mismo tiempo puede ponerse a disposición del usuario del equipo de procesamiento de datos adicional, que quiere hacer uso de un servicio relevante con respecto a la seguridad, como banca en línea, la clave asignada a este usuario. Preferiblemente se pone a disposición del usuario la clave en otra vía de comunicación o al menos con un retardo en el tiempo.

Entonces, por medio de la clave personalizada el usuario puede descifrar el paquete de datos y en particular ejecutar el programa de acceso a red. Entonces el usuario puede realizar los servicios relevantes con respecto a la seguridad deseados con el navegador web. Más abajo se realiza una descripción detallada del procedimiento.

La figura 2 muestra un diagrama de bloques de una forma de realización a modo de ejemplo de un sistema con una forma de realización a modo de ejemplo de un primer equipo (200) de procesamiento de datos. Como ya se describió anteriormente, el equipo (200) de procesamiento de datos puede ser un servidor o un componente de servidor. Este equipo de procesamiento de datos puede proporcionarse por el proveedor de los servicios relevantes con respecto a la seguridad. Por ejemplo, un banco puede poner a disposición un servidor correspondiente para la realización de banca en línea.

El primer equipo (200) de procesamiento de datos puede comprender un procesador (270) configurado como microprocesador, una microunidad de control como microcontrolador, un procesador digital de señales (DSP), un circuito integrado de aplicación específica (ASIC) o una disposición de puertas programables en campo (FPGA).

Este procesador puede ejecutar por ejemplo instrucciones de programa, que están almacenadas en memorias de programa y almacena por ejemplo resultados intermedios o similares en la memoria principal. Por ejemplo, la memoria de programa es una memoria de sólo lectura (ROM) y la memoria principal es una memoria volátil o no volátil, en particular una memoria con acceso aleatorio (RAM) y/o una memoria flash.

Además el equipo (200) de procesamiento de datos puede comprender un dispositivo (280) de soporte de datos, que por ejemplo puede ser un medio de almacenamiento legible por ordenador, que presenta un programa (282) informático según la invención, que puede ejecutarse mediante el procesador (270).

El primer equipo (200) de procesamiento de datos a modo de ejemplo comprende además un generador (202) de autenticación, un generador (204) de paquete de datos, un generador (206) de clave y un generador (208) de cifrado.

El generador (202) de autenticación está configurado para generar la al menos una característica (212) de autenticación personalizada. El generador (204) de paquete de datos genera el paquete (210) de datos, uniendo los componentes (212, 214 y 216) individuales del paquete (210) de datos.

El generador (206) de clave genera la clave (218) personalizada. Esta clave (218) se utiliza por el generador (208) de cifrado para cifrar el paquete (210) de datos. El generador (208) de cifrado puede presentar además un módulo de compresión para comprimir el paquete (210) de datos. Se entiende que el módulo de compresión según otras

variantes de la invención también puede estar formado como módulo separado del primer equipo (200) de procesamiento de datos.

Además, de la figura 2 puede deducirse que el primer equipo (200) de procesamiento de datos puede presentar dos módulos (220 y 230) de transmisión. El módulo (220) de transmisión puede ser en particular un módulo (220) de transmisión de clave para transmitir la clave (218) personalizada al usuario (260, 262) correspondiente a través de una vía (221) de comunicación que puede establecerse.

El módulo (230) de transmisión adicional puede ser preferiblemente un módulo (230) de transmisión de paquete de datos para transmitir el paquete (210) de datos individualizado al usuario (260, 262) correspondiente o su equipo (240) de procesamiento de datos adicional a través de una vía (231) de comunicación adicional que puede establecerse.

Además, el primer equipo (200) de procesamiento de datos comprende un equipo (250) de memoria en forma de base (250) de datos. En la base (250) de datos pueden almacenarse de manera centralizada por ejemplo datos para la autenticación. Así por ejemplo pueden depositarse las características (212) de autenticación personalizadas con los datos de usuario correspondientes, como nombre, dirección, etc. Adicionalmente pueden almacenarse las claves (218) personalizadas. Se entiende que la base (250) de datos no tiene que estar dispuesta directamente en el primer equipo (200) de procesamiento de datos, sino que también puede estar dispuesta de manera remota, siempre que el primer equipo (200) de procesamiento de datos pueda acceder a la base (250) de datos.

Como ya se mencionó, como equipos (240) de procesamiento de datos adicionales pueden utilizarse ordenadores, portátiles, teléfonos inteligentes y similares. Estos aparatos (240) pueden presentar una memoria (242) volátil, como por ejemplo una memoria (242) de trabajo.

La función del sistema representado en la figura 2 se explica a continuación en más detalle con ayuda de la figura 3.

La figura 3 muestra un segundo diagrama de flujo con etapas de procedimiento de una forma de realización a modo de ejemplo de la invención.

En una primera etapa (302) el generador (202) de autenticación puede generar una característica (212) de autenticación personalizada, que está asignada a un único usuario (260, 262). Por ejemplo se genera una contraseña o un certificado adecuado, que es unívoco.

Además, según la presente forma de realización se pone a disposición un programa (214) de acceso a red protegido, que está configurado especialmente para el servicio relevante con respecto a la seguridad deseado (etapa 304).

En una etapa (306) adicional puede proporcionarse una configuración (216), por ejemplo en forma de un archivo (216) de configuración. El archivo (216) de configuración puede establecer la configuración del programa (214) de acceso a red al ejecutar el programa (214) de acceso a red. El archivo (216) de configuración se explica a continuación en más detalle.

Como puede deducirse de la figura 3, las etapas (302, 304, 306) de procedimiento pueden realizarse preferiblemente de manera paralela. Sin embargo, se entiende que según otras variantes de la invención también es posible un desarrollo en serie de estas etapas.

Después de haber generado o haber puesto a disposición los componentes (212, 214 y 216), en una siguiente etapa (308) puede generarse el paquete (210) de datos mediante el generador (204) de paquete de datos. Así pueden unirse los componentes (212, 214 y 216) individuales y en particular unirse entre sí de manera firme, para evitar una separación posterior. De este modo se reduce adicionalmente el riesgo de manipulaciones del programa (214) de acceso a red. En particular se genera un paquete (210) de datos personalizado, que exclusivamente está asignado a un usuario (260, 262).

Entonces el generador (206) de clave, en una siguiente etapa (310), puede generar una clave (218) personalizada. La clave (218) asignada al usuario (260, 262) puede ser un código de activación o una contraseña. Se entiende que la clave (218) también puede generarse de manera paralela a una de las etapas (302 a 308) de procedimiento anteriores.

Preferiblemente el paquete (210) de datos puede comprimirse en la siguiente etapa (312) y cifrarse con la clave (218) personalizada generada anteriormente mediante el generador (208) de cifrado. La compresión y el cifrado pueden realizarse según otras variantes de la invención también en serie. Además las etapas de unión, cifrado y compresión pueden realizarse juntas mediante un generador correspondiente. Por ejemplo con un generador de archivos ZIP es posible generar un archivo ZIP.

Sin embargo, también es concebible que el paquete de datos en la etapa (312) sólo se cifre y no tenga lugar una compresión del paquete de datos.

El cifrado con la clave (218) personalizada provoca que un descifrado del paquete (210) de datos sólo sea posible con ayuda de la clave (218), que preferiblemente es unívoca.

En una etapa (314) adicional la característica (212) de autenticación asignada al usuario (260, 262), los datos del usuario (260, 262) y/o la clave (218) personalizada pueden almacenarse y preferiblemente depositarse en una base (250) de datos. Se entiende también en este caso que el almacenamiento de los datos en principio puede producirse en cualquier momento, en particular directamente tras la generación de los datos.

La clave (218) personalizada generada y el paquete (210) de datos personalizado generado pueden transmitirse entonces al usuario (260, 262) correspondiente o su equipo (240) de procesamiento de datos adicional (etapas (316 y 318)). Los dos componentes (210 y 218) pueden transmitirse tanto al mismo tiempo como sucesivamente. Preferiblemente, el paquete (210) de datos se transmite a través de otra vía (231) de comunicación que la de la clave (218). Por ejemplo, el paquete (210) de datos puede ponerse a disposición por el módulo (230) de transmisión para una descarga o el paquete (210) de datos puede almacenarse en un soporte de datos, como un DVD, CD o similares y transmitirse al usuario (260, 262). Por el contrario, la clave (218) personalizada puede transmitirse por correo electrónico, SMS, correo o similares. A través de las vías (221, 231) de comunicación separadas a un atacante potencial se le dificulta de manera significativa averiguar los datos relevantes con respecto a la seguridad.

En una siguiente etapa (320) el usuario (260, 262) recibe directa o indirectamente a través de su equipo (240) de procesamiento de datos adicional el paquete (210) de datos y la clave (218). Se entiende que el momento de recepción real de los dos componentes (210, 218) puede diferir.

En una siguiente etapa (322) el usuario (260, 262) inicia el paquete (210) de datos y según el presente ejemplo de realización en la etapa (324) se le solicita la introducción de la clave (218) personalizada. La introducción puede producirse mediante aparatos de interfaz adecuados, como un teclado, una pantalla táctil o similares.

Cuando la clave (218) personalizada corresponde al paquete (210) de datos cifrado, entonces en la siguiente etapa (326) puede descifrarse el paquete (210) de datos y dado el caso descomprimirse. En caso contrario, puede producirse un mensaje de error y puede pedirse al usuario (260, 262) que vuelva a introducir la clave (218) personalizada.

El descifrado y la descompresión pueden realizarse preferiblemente al mismo tiempo. En particular, esta operación de desempaquetado y descifrado puede realizarse directamente en la memoria (242) de trabajo del ordenador (240) operativo. En este caso no están visibles archivos no cifrados como resultado intermedio. Se dificulta adicionalmente una manipulación del navegador (214) web protegido.

Después de que el paquete (210) de datos esté descomprimido y descifrado, el navegador (214) web protegido puede ejecutarse preferiblemente sin instalación (etapa (326)). A este respecto el navegador (214) web puede tener acceso a la característica (212) de autenticación personalizada.

Alternativamente también es concebible, por ejemplo cuando el paquete (210) de datos en la etapa (312) no se ha comprimido, que en la etapa (326) sólo tenga lugar un descifrado del paquete (210) de datos. Preferiblemente, el paquete (210) de datos se descifra a este respecto directamente en la memoria (242) de trabajo del ordenador (240) y el navegador (214) web protegido se ejecuta directamente desde la memoria (242) de trabajo del ordenador (240).

Entonces, el usuario (260, 262) o bien puede abrir él mismo una página de Internet en el navegador (214) web, o bien puede abrirse automáticamente al iniciar el navegador (214) web a través de su archivo (216) de configuración (etapa (326)). Igualmente, dentro del archivo (216) de configuración del navegador (214) web pueden encontrarse ajustes correspondientes para verificar la autenticidad de la página de Internet solicitada, por ejemplo en forma de certificados SSL.

En una siguiente etapa (330) el usuario (260, 262) por medio de la característica (212) de autenticación personalizada puede autenticarse con respecto a la página de Internet, que se pone a disposición por ejemplo por el primer equipo (200) de procesamiento de datos. A este respecto puede realizarse una comparación de la característica (212) de autenticación con los datos depositados en la base (250) de datos. A este respecto puede solicitarse opcionalmente al usuario (260, 262) la nueva introducción de su clave (218) personalizada o de una clave personalizada adicional para descifrar la característica (212) de autenticación personalizada. Tras un resultado de autenticación positivo el usuario (260, 262) puede realizar el servicio relevante con respecto a la seguridad deseado, como por ejemplo una transferencia o similares, con el programa de acceso a red concebido exclusivamente para este fin. En caso de que la autenticación lleve a un resultado negativo, entonces se evita una ejecución del programa (214) de acceso a red y en particular una realización del servicio relevante con respecto a la seguridad.

Durante todo el tiempo de ejecución del programa (214) de acceso a red la función de protección del programa (214) de acceso a red puede supervisar su estado. A este respecto puede supervisarse en particular que ningún otro proceso intenta engancharse en el espacio de proceso del programa (214) de acceso a red (por ejemplo mediante depuradores, hilos remotos o enlace), para manipular su comportamiento, desactivar la función de protección o leer la característica (212) de autenticación personalizada o la clave (218) personalizada. Además, el navegador (214) web antes de realizar o liberar un servicio relevante con respecto a la seguridad puede comunicar datos cifrados al primer equipo (200) de procesamiento de datos. Estos datos pueden comprender por ejemplo el estado del navegador (214) web, en particular el estado interno, un sello de fecha y hora y datos aleatorios. Mediante la detección y comunicación del estado interno del navegador puede evitarse una inyección de código.

En una última etapa (332), tras la realización del servicio relevante con respecto a la seguridad, puede finalizarse el programa (214) de acceso a red y en particular volver a comprimirse y cifrarse automáticamente.

En caso de que el usuario (260, 262) desee realizar una transacción adicional relevante con respecto a la seguridad, entonces puede volver a iniciar el programa (214) de acceso a red (etapa (322)).

Para poner a disposición de usuarios (262) adicionales igualmente un paquete (210) de datos personalizado y cifrado, puede volver a iniciarse el procedimiento con las etapas (302, 304 y 306).

Puede estar previsto que cada vez que el usuario desee realizar una transacción segura (por ejemplo banca en línea), inicie el archivo empaquetado individualmente para él y al inicio introduzca su clave individual de usuario. A continuación, el navegador web, incluidas la función de protección y la característica de autenticación individual para el usuario, puede descifrarse a partir de la función de empaquetado de cifrado con ayuda de la clave individual de usuario y desempaquetarse. Esta operación de desempaquetado y descifrado puede realizarse de manera ideal directamente en la memoria de trabajo del ordenador operativo, de modo que no estén visibles archivos no cifrados como resultado intermedio. El navegador web puede ejecutarse junto con la función de protección y tiene acceso a la característica de autenticación individual del usuario.

Además también puede estar previsto un componente de servidor que a partir de los componentes individuales de navegador web y una función de empaquetado cree el archivo individual de usuario, en el que con ayuda de un generador de característica de autenticación se incluye la característica de autenticación individual de usuario. Los componentes mencionados pueden empaquetarse entonces con ayuda de la función de empaquetado en el archivo individual de usuario y cifrarse con la clave individual de usuario. La clave individual de usuario puede haberse generado anteriormente por el generador de clave. Puede proporcionarse al usuario por una vía separada, por ejemplo por SMS o carta certificada.

Mediante la invención, el usuario obtiene un navegador web protegido individual que ofrece menos posibilidades de ataque que el navegador web existente habitualmente en los ordenadores de usuario. Además el navegador web protegido está unido estrechamente con una característica de autenticación mediante el cifrado.

A diferencia del estado de la técnica según la invención la autenticación de 2 factores puede realizarse sin hardware como solución de software pura. Para ello puede utilizarse un software personalizado, que está configurado individualmente para cada usuario. Así, un usuario puede obtener inicialmente de un proveedor de servicios, como un banco, un código de activación por SMS o correo electrónico. Entonces, el usuario puede registrarse en el banco con su nombre de usuario y una contraseña y por medio del código de activación descargarse el programa de acceso a red personalizado, en particular un navegador. El programa de acceso a red puede ocultarse por medio de un ofuscador y dotarse de una “marca de agua”. Ahora, el usuario puede utilizar este navegador seguro para los servicios en línea, autenticando el banco al usuario cuando éste se registra como se describió anteriormente y el navegador envía la marca de agua, es decir, la característica de autenticación, al banco.

Por ejemplo, puede empaquetarse un único paquete de datos que puede ejecutarse, que comprende un navegador con función de protección, como mecanismos contra ingeniería de inversión, contra depuración, contra registrador de teclas (*Anti-Keylogger*) y contra inyección de código, pudiendo estar individualizado este paquete para cada usuario. Puede estar previsto un mecanismo contra registrador de teclas para evitar que se intercepte la contraseña o el código de activación del usuario de un atacante. El navegador puede activarse mediante un código de activación unívoco, como una contraseña, de modo que se descifran al menos partes del navegador y puede ejecutarse el navegador. El navegador, antes de realizar o liberar el navegador, puede comunicar datos cifrados al primer equipo de procesamiento de datos. Estos datos pueden comprender por ejemplo el estado del navegador web, en particular el estado interno, un sello de fecha y hora y datos aleatorios. Mediante la detección y comunicación del estado interno del navegador puede evitarse una inyección de código.

La sucesión de las etapas de procedimiento individuales en los diagramas de flujo individuales no es obligatoria, son concebibles sucesiones alternativas de las etapas de procedimiento. Las etapas de procedimiento pueden implementarse de diferente manera, así es concebible una implementación en software (mediante instrucciones de programa), hardware o una combinación de ambos para la implementación de las etapas de procedimiento.

Las formas de realización de la presente invención detalladas a modo de ejemplo, descritas en esta solicitud también se dan a conocer en todas las combinaciones entre sí.

**REIVINDICACIONES**

1. Procedimiento, que comprende:

- generar un paquete (210) de datos que comprende al menos un programa (214) de acceso a red protegido y al menos una característica (212) de autenticación personalizada en un primer equipo (200) de procesamiento de datos, en el que el paquete de datos comprende la al menos una característica de autenticación personalizada junto al al menos un programa de acceso a red, y en el que el paquete (210) de datos es un paquete de datos formado por un gran número de paquetes de datos adaptados individualmente a respectivos usuarios (260, 262), que comprenden en cada caso el programa (214) de acceso a red y una característica de autenticación personalizada asignada al respectivo usuario,

- generar una clave (218) personalizada,

- cifrar el paquete (210) de datos para asociar la característica (212) de autenticación personalizada con el programa (214) de acceso a red, y

- proporcionar el paquete (210) de datos para una transmisión a un equipo (240) de procesamiento de datos adicional, en el que el paquete (210) de datos transmitido puede descifrarse con la clave (218) personalizada introducida por un usuario en el equipo (240) de procesamiento de datos adicional, de tal manera que el programa (214) de acceso a red puede ejecutarse, con ello el programa (214) de acceso a red tiene acceso a la característica (212) de autenticación personalizada y puede autenticarse mediante la característica (212) de autenticación personalizada.

2. Procedimiento según la reivindicación 1, en el que el paquete de datos está asignado a un único usuario, y en el que la característica de autenticación personalizada sirve para verificar si el programa de acceso a red o el usuario del programa de acceso a red está autorizado para la realización de un servicio relevante con respecto a la seguridad.

3. Procedimiento según una de las reivindicaciones anteriores, en el que el programa (214) de acceso a red y la característica (212) de autenticación pueden descifrarse en una zona de una memoria (242) de trabajo de la instalación (240) de procesamiento de datos y pueden ejecutarse desde la memoria (242) de trabajo, de tal manera que el programa de acceso a red descifrado y la característica de autenticación descifrada durante la ejecución del programa (214) de acceso a red sólo están almacenados en la memoria (242) de trabajo y no tiene lugar un almacenamiento del programa (214) de acceso a red descifrado y de la característica (212) de autenticación descifrada en un disco duro del equipo (240) de procesamiento de datos.

4. Procedimiento según una de las reivindicaciones anteriores, en el que el paquete (210) de datos comprende al menos un archivo (216) de configuración, y en el que el archivo (216) de configuración establece la configuración del programa (214) de acceso a red al ejecutar el programa (214) de acceso a red.

5. Procedimiento según una de las reivindicaciones anteriores, en el que el programa de acceso a red protegido está configurado especialmente para un servicio relevante con respecto a la seguridad.

6. Procedimiento según una de las reivindicaciones anteriores, en el que el paquete (210) de datos y la clave (218) personalizada correspondiente se transmiten por separado.

7. Procedimiento según una de las reivindicaciones anteriores, en el que el programa (214) de acceso a red se modifica al menos parcialmente de manera personalizada.

8. Procedimiento según una de las reivindicaciones anteriores, que comprende además:

- asignar la característica (212) de autenticación personalizada del paquete (210) de datos y de la clave (218) personalizada correspondiente al paquete (210) de datos a un usuario (260, 262), y

- almacenar la asignación en una base (250) de datos del primer equipo (200) de procesamiento de datos.

9. Procedimiento según una de las reivindicaciones anteriores, que comprende además autenticar un usuario (260, 262) del equipo (240) de procesamiento de datos adicional con respecto al primer equipo (200) de procesamiento de datos por medio de la característica (212) de autenticación personalizada, de tal manera que el usuario (260, 262) pueda realizar un servicio relevante con respecto a la seguridad exclusivamente en caso de autenticación positiva.

10. Procedimiento según una de las reivindicaciones anteriores, en el que la característica de autenticación es un certificado de software y/o una contraseña.

11. Procedimiento según una de las reivindicaciones anteriores, en el que el paquete (210) de datos es un paquete de datos que puede ejecutarse.

12. Procedimiento según una de las reivindicaciones anteriores, que comprende además

- descifrar el paquete (210) de datos en una memoria (242) volátil del equipo (240) de procesamiento de datos adicional, y/o

- ejecutar el programa (214) de acceso a red directamente desde la memoria (242) volátil del equipo (240) de procesamiento de datos adicional.

13. Programa (282) informático, que comprende instrucciones de programa que permiten que un procesador (270) realice el procedimiento según una de las reivindicaciones 1 a 11, cuando el programa (282) informático se ejecuta en el procesador (270).

14. Equipo (200) de procesamiento de datos, que comprende

- medios para la realización del procedimiento según una de las reivindicaciones 1-11.

15. Sistema que comprende

- un equipo (200) de procesamiento de datos según la reivindicación 14, y

- al menos el equipo (240) de procesamiento de datos adicional.

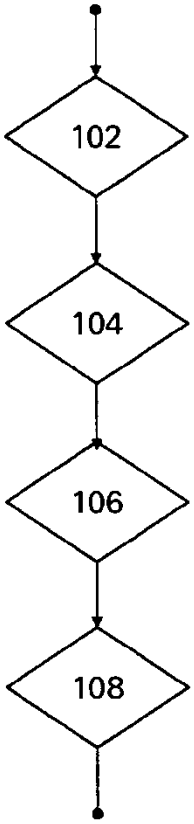
102
104
106
108

Fig. 1

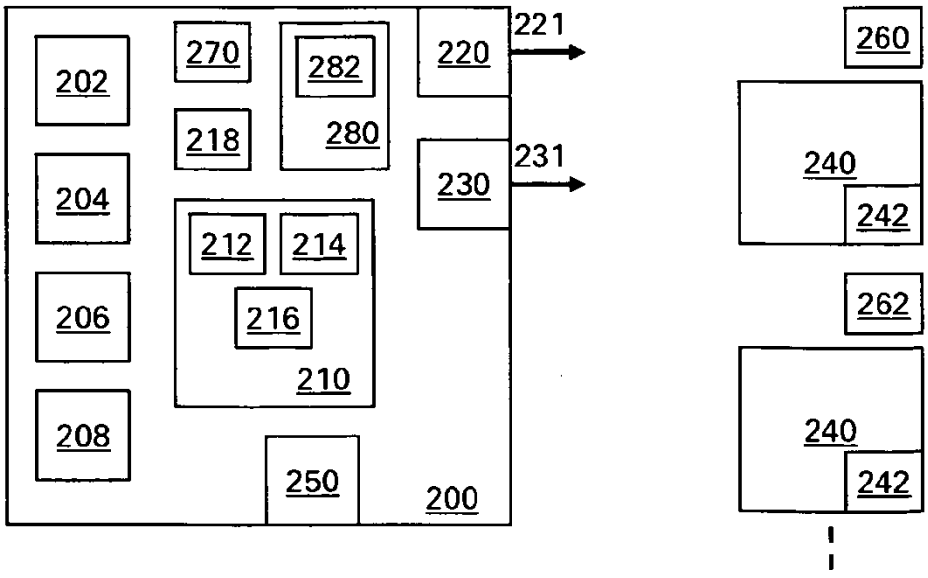
202
270
282
220
221
218
280
204
230
231
212
214
216
206
210
208
250
200
260
240
242
262
240
242

Fig. 2

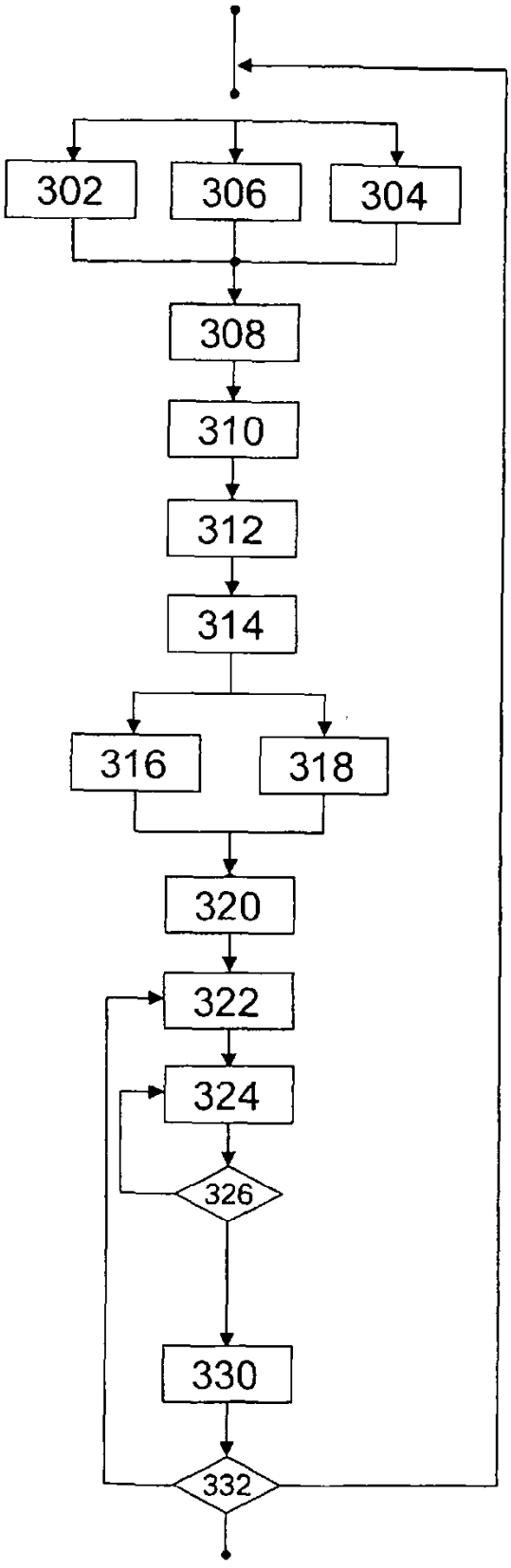


Fig. 3 modificada