(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 662 897**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.07.2016 E 16180092 (5)**

(97) Fecha y número de publicación de la concesión europea: **24.01.2018 EP 3125492**

(54) Título: **Procedimiento y sistema para generar un canal de comunicación seguro para aparatos terminales**

(30) Prioridad:

28.07.2015 DE 102015214267

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.04.2018

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Wittelsbacherplatz 2
80333 München, DE

(72) Inventor/es:

FRIES, STEFFEN y
SCHAFHEUTLE, MARCUS

(74) Agente/Representante:

LOZANO GANDIA, José

PROCEDIMIENTO Y SISTEMA PARA GENERAR UN CANAL DE COMUNICACIÓN SEGURO PARA APARATOS TERMINALES

DESCRIPCIÓN

La invención se refiere a un procedimiento y un sistema para generar un canal de comunicación seguro para aparatos terminales.

Las credenciales de seguridad (en inglés Security Credentials), como en particular certificados digitales, un token de seguridad (en inglés Security Token) o un ticket de seguridad (en inglés Security Ticket), se necesitan para apoyar servicios de seguridad en determinados escenarios. Tales servicios de seguridad pueden ser por ejemplo el establecimiento de un canal de comunicación entre dos interlocutores o también el transporte de un ticket de licencia entre dos o tres participantes. Usualmente proporciona una infraestructura de seguridad una tal credencial de seguridad.

En una aplicación específica, que incluye la comunicación entre tres participantes, existe la necesidad de asegurar que una credencial de seguridad por un lado se ha transportado correctamente de forma criptográfica, pero también a través de un canal de comunicación asegurado.

Se conocen los siguientes documentos:

US 2014/0075198 da a conocer un procedimiento convencional para la transmisión autentificada de datos de video u otros datos desde un proveedor a un aparato receptor a través de un aparato de transmisión.

US 2012008784 da a conocer un procedimiento convencional de intercambio de claves.

El objetivo de la invención es proporcionar un canal de comunicación seguro para transportar una credencial de seguridad.

Según un primer aspecto se refiere la invención a un procedimiento para generar un canal de comunicación seguro para un aparato terminal. El procedimiento incluye una etapa del procedimiento para establecer un canal de comunicación seguro mediante un protocolo de comunicación entre un interlocutor de comunicación y un back-end (terminal del lado del servidor) fijándose en cada caso una información de enlace del canal para el back-end y para el interlocutor de comunicación mediante el protocolo de comunicación. El procedimiento incluye una etapa del procedimiento para generar un canal de comunicación entre el interlocutor de comunicación y el aparato terminal. El procedimiento incluye una etapa del procedimiento para transmitir la información de enlace del canal relativo al canal de comunicación seguro por medio del interlocutor de comunicación al aparato terminal. El procedimiento incluye una etapa del procedimiento para memorizar la información de enlace del canal en el aparato terminal. El procedimiento incluye una etapa del procedimiento para confeccionar una estructura de datos y una primera firma digital mediante la estructura de datos por medio del back-end con una primera clave privada, pudiendo comprobarse la primera firma digital con una primera clave pública. El procedimiento incluye una etapa del procedimiento para enviar la estructura de datos y la primera firma digital desde el back-end al aparato terminal. El procedimiento incluye una etapa del procedimiento para comprobar la autenticidad de la estructura de datos mediante un algoritmo de prueba para verificar la primera firma digital mediante la primera clave pública por parte del aparato terminal y/o por parte del interlocutor de comunicación.

Bajo un “back-end” puede entenderse en el contexto de la invención por ejemplo una unidad procesadora de datos de cualquier tipo, en particular unidades procesadoras de datos con funcionalidades de cliente y/o funcionalidades de servidor. Un back-end es por ejemplo, contrariamente a un Front-End (terminal del lado del usuario), una parte de un sistema de computadora (implementado por ejemplo como arquitectura cliente-servidor), que en particular está alejada del usuario. En particular se encuentra el mismo, cuando se observa, más próximo al sistema y por el contrario el front-end está más próximo al usuario. En una arquitectura cliente-servidor por ejemplo constituye el back-end el servidor que alimenta los clientes.

Bajo un "canal de comunicación" puede entenderse en el contexto de la invención por ejemplo un canal de comunicación en forma de un enlace de comunicación inalámbrico y/o un enlace de comunicación por línea física y/o una comunicación a través de un conductor de fibra óptica y/o una comunicación análoga (por ejemplo cartas).

Bajo un "interlocutor de comunicación" puede entenderse en el contexto de la invención por ejemplo una Workstation (terminal de trabajo) con una herramienta de programación y/o una computadora de un audiólogo y/o un aparato de configuración para el aparato terminal.

El procedimiento permite establecer un canal de comunicación seguro para el aparato terminal hasta el back-end e intercambiar la estructura de datos. En particular ofrece el procedimiento la ventaja de establecer un canal de comunicación seguro para aparatos terminales que por sí mismos disponen de reducidas capacidades de cálculo y que sólo pueden establecer canales de comunicación sin proteger

criptográficamente. El interlocutor de comunicación sirve así al aparato terminal como un puente seguro hasta el back-end. Las informaciones de enlace del canal pueden aquí ser idénticas para el back-end y para el interlocutor de comunicación. Pero también es posible que las informaciones de enlace del canal para el back-end y para el interlocutor de comunicación sean diferentes, pero tengan una inequívoca relación entre sí mediante una función matemática.

En una primera forma de realización del procedimiento presenta el procedimiento una etapa de procedimiento adicional para enviar informaciones de seguridad y/o informaciones de identidad desde el aparato terminal a través del interlocutor de comunicación al back-end, presentando el envío de informaciones de seguridad y/o informaciones de identidad desde el aparato terminal a través del interlocutor de comunicación al back-end en particular las siguientes etapas del procedimiento: Una etapa del procedimiento para enviar informaciones de seguridad e informaciones de identidad desde el aparato terminal al interlocutor de comunicación y una etapa del procedimiento para enviar las informaciones de seguridad e informaciones de identidad del aparato terminal desde el interlocutor de comunicación a través del canal de comunicación seguro al back-end.

De esta manera es posible enviar informaciones críticas para la seguridad del aparato terminal a través del canal de comunicación seguro del interlocutor de comunicación al back-end.

En otras formas de realización del procedimiento incluye la estructura de datos la información de enlace del canal y/o informaciones básicas del back-end.

La ventaja reside en la inclusión de una identificación inequívoca en forma de las informaciones de enlace del canal para el canal de comunicación seguro entre el back-end y el interlocutor de comunicación. Puesto que el canal de comunicación seguro entre el back-end y el interlocutor de comunicación se estableció según una directriz de seguridad prescrita del back-end y mediante la información de enlace del canal se une a la comunicación con el aparato terminal, hay una relación directa de seguridad entre back-end y aparato terminal. De esta manera es posible asegurar por el lado del aparato terminal y también por el lado del back-end que una información de configuración, por ejemplo un ticket de licencia, se ha transportado a través de un canal de comunicación previamente establecido que se estableció según una directriz de seguridad del back-end.

En otras formas de realización del procedimiento se proporciona una señal a través del aparato terminal y/o a través del interlocutor de comunicación, cuando el algoritmo de prueba detecta una autenticidad no válida.

Mediante la señal, que puede contener una información de control, pueden informarse por ejemplo a un usuario cuando se haya detectado una autenticidad no válida. En un caso así, el usuario puede por ejemplo finalizar el enlace, para evitar que se transmitan informaciones críticas para la seguridad. Pero también es posible que mediante la señal se supriman conscientemente avisos de falta o también conscientemente se mantengan en general.

En otras formas de realización del procedimiento se proporciona la primera clave pública para el aparato terminal, proporcionando en particular una entidad certificadora o el back-end la primera clave pública.

De esta manera se proporciona de la manera más sencilla posible la primera clave pública al aparato terminal.

En otras formas de realización del procedimiento incluyen las informaciones de base del back-end una información de configuración, incluyendo la información de configuración en particular una información de licencia y/o código de programa para ejecutar una orden que lleva a cabo el aparato terminal sobre el aparato terminal.

De esta manera puede transmitirse por ejemplo, de la forma más protegida posible, una información de licencia, por ejemplo un ticket de licencia, al aparato terminal, para liberar por ejemplo nuevas funciones de aparato sobre el aparato terminal.

En otras formas de realización del procedimiento dispone el aparato terminal de un segundo par de claves en forma de una segunda clave pública y una segunda clave privada, con la que se genera para las informaciones de seguridad del aparato terminal una segunda firma digital.

De esta manera pueden protegerse criptográficamente las informaciones de seguridad. El segundo par de claves o bien el procedimiento criptográfico utilizado es entonces independiente de la primera clave privada y de la primera clave pública que forman un primer par de claves. Así pueden elegirse en cada caso fortalezas de clave distintas y procedimientos criptográficos de distinta fortaleza. En particular pueden por ejemplo utilizar así aparatos terminales con reducidas capacidades de cálculo un procedimiento criptográfico débil y utilizarse entre el interlocutor de comunicación y el back-end un procedimiento criptográfico claramente más fuerte.

En otras formas de realización del procedimiento, comprueba el interlocutor de comunicación una segunda autenticidad de la información de seguridad mediante la segunda clave pública y la segunda firma digital.

De esta manera le resulta posible al interlocutor de comunicación comprobar la autenticidad de la segunda firma digital. Si detecta el mismo que la segunda firma digital es inválida, puede él por ejemplo finalizar el enlace con el aparato terminal y/o back-end, para que en particular no llegue ninguna información crítica para la seguridad a terceros no autorizados.

En otras formas de realización del procedimiento incluye la información de seguridad un nonce (number used once, número que sólo puede usarse una vez) y/o un identificador de un certificado del aparato terminal y/o sólo una huella digital de la segunda clave pública.

Las informaciones adicionales contenidas en las informaciones de seguridad permiten que la comunicación entre el aparato terminal y el back-end sea aún más segura. Por ejemplo se utiliza el nonce para evitar ataques de replay (de reproducción). El nonce puede generarse por ejemplo mediante un generador de aleatoriedad o como parte de un protocolo de comunicación criptográfica.

En otras formas de realización del procedimiento, se incluye la información de seguridad y/o la información de enlace del canal y/o las informaciones de identidad, total o parcialmente, en la primera firma digital.

La inclusión de la información de enlace del canal en la firma digital tiene en particular la ventaja de que el aparato terminal puede comprobar la existencia de un canal de comunicación seguro entre back-end e interlocutor de comunicación. Esto es posible, ya que el interlocutor de comunicación ha transmitido su información de enlace del canal al aparato terminal y el back-end ha archivado igualmente su información de enlace del canal en la primera firma digital. Puesto que mediante la primera firma digital está protegida criptográficamente la información de enlace del canal correspondiente al back-end, queda asegurado que puede detectarse una manipulación. El aparato terminal compara la información de enlace del canal y rechazaría en una manipulación del enlace, por ejemplo un Session Hijacking (secuestro de la sesión), la ejecución de una información de configuración. Mediante el procedimiento es posible que un aparato terminal débil en cuanto a cálculo, que sólo dispone de mecanismos de protección criptográficos débiles, pueda aprovechar no obstante las ventajas de un canal de comunicación protegido fuertemente de forma criptográfica.

En otras formas de realización del procedimiento incluye la estructura de datos y/o la primera firma digital una información de legitimidad, que da lugar a que el aparato terminal conecte en particular una determinada programación.

Mediante el procedimiento es posible que un aparato terminal débil en cuanto a cálculo, que sólo dispone de mecanismos de protección criptográficos débiles, pueda aprovechar no obstante las ventajas de un canal de comunicación protegido fuertemente de forma criptográfica. En particular está protegida la información de legitimidad por la primera firma digital.

En otras formas de realización del procedimiento se amplía la estructura de datos en la primera firma digital.

De esta manera se logra simplificar aún más el manejo de los datos. En detalle, se amplía la estructura de datos anexando la primera firma digital y se envía como una unidad.

En otras formas de realización del procedimiento incluye la estructura de datos adicionalmente las informaciones de seguridad y/o informaciones de identidad del aparato terminal.

Mediante la inclusión por ejemplo de la información de identidad en la estructura de datos, puede llevarse por ejemplo a un estado seguro un aparato terminal para el que se ha detectado una manipulación de un enlace de comunicación, para evitar más manipulaciones.

En otras formas de realización del procedimiento comprueba el algoritmo de prueba para detectar la autenticidad, adicionalmente la información de enlace del canal memorizada y la información de enlace del canal, ejecutándose el algoritmo de prueba en particular en el aparato terminal y/o en el interlocutor de comunicación.

La ventaja de la inclusión de la información de enlace del canal en la primera firma digital y/o la estructura de datos es que el aparato terminal puede comprobar la existencia del canal de comunicación seguro entre back-end e interlocutor de comunicación. Esto es posible ya que el interlocutor de comunicación ha transmitido su información de enlace del canal al aparato terminal y el back-end igualmente ha archivado su información de enlace del canal en la primera firma digital. Puesto que mediante la primera firma digital queda protegida criptográficamente la información de enlace del canal del back-end, queda asegurado que puede detectarse una manipulación. El aparato terminal compara la información de enlace del canal y

cuando existiera una manipulación del enlace, por ejemplo un hijacking (secuestro) de la sesión, rechazaría la ejecución de una información de configuración. Mediante el procedimiento es por lo tanto posible que un aparato terminal débil en cuanto a cálculo, que sólo dispone de mecanismos de protección criptográficamente débiles, pueda aprovechar no obstante las ventajas de un canal de comunicación protegido fuertemente de forma criptográfica.

En otras formas de realización del procedimiento envía el interlocutor de comunicación, en el envío de informaciones de seguridad e informaciones de identidad desde el interlocutor de comunicación al back-end, informaciones adicionales, incluyendo las informaciones adicionales en particular una información de usuario.

Mediante la inclusión por ejemplo de la información de usuario, puede informarse en particular a un usuario que desea programar el aparato terminal y que ha solicitado para el aparato terminal una información de base, estructura de datos y/o información de configuración, por ejemplo una información de licencia, para liberar nuevas funciones en el aparato terminal, sobre una potencial manipulación del enlace de comunicación con el back-end.

En otras formas de realización del procedimiento, cuando se envía la estructura de datos se envía a la vez la primera clave pública.

De esta forma puede proporcionarse de manera especialmente sencilla la primera clave pública al aparato terminal.

En otra forma de realización comprueba el interlocutor de comunicación la primera clave pública antes de retransmitir la primera clave pública al aparato terminal, siendo la clave pública en particular un certificado, validándose el certificado en particular frente a un expedidor conocido, incluyendo la validación del certificado en particular una validez y/o un estado de rechazo.

En otras formas de realización del procedimiento se proporciona la primera clave pública en un instante más temprano al aparato terminal, siendo el instante más temprano en particular el momento de la fabricación del aparato terminal, estando protegida la primera clave pública en particular contra una modificación en el aparato terminal.

De esta manera puede archivarse por ejemplo la primera clave pública en una memoria protegida frente a lectura y/o escritura del aparato terminal durante la fabricación. Cuando por ejemplo esta archivada la primera clave pública en una memoria de sólo lectura, por ejemplo ROM (Read Only Memory) o bien WORM (Write Once Read Memory, memoria de una sola escritura y lecturas múltiples), está especialmente protegida ésta frente a manipulaciones.

En otras formas de realización del procedimiento la primera clave privada es un secreto que el back-end conoce, siendo conocido el secreto en particular exclusivamente por el back-end.

De esta manera se logra una elevada seguridad, ya que sólo el back-end está en condiciones de confeccionar una primera firma digital válida.

En otra forma de realización del procedimiento dispone el aparato terminal sólo de informaciones no críticas para la seguridad.

El procedimiento puede utilizarse en particular para aparatos terminales con ninguna o pocas funciones de seguridad o bien funciones criptográficas. Esto tiene en particular la ventaja de que estos aparatos terminales no obstante pueden utilizar un canal de comunicación que está fuertemente protegido criptográficamente.

En otras formas de realización del procedimiento se genera el canal de comunicación seguro mediante un procedimiento simétrico, utilizando el procedimiento simétrico en particular una autentificación con un nombre de usuario y una palabra de paso o bien el canal de comunicación seguro se genera mediante un procedimiento asimétrico, utilizando el procedimiento asimétrico en particular un certificado digital.

Mediante la posibilidad de utilizar distintos procedimientos criptográficos, puede utilizarse el procedimiento de acuerdo con la invención por ejemplo para distintas infraestructuras de seguridad.

En otras formas de realización del procedimiento, la señal es evaluada por el back-end u otro interlocutor de comunicación.

Mediante la evaluación de la señal puede comprobarse por ejemplo en el otro interlocutor de comunicación, por ejemplo una estación de seguridad, qué aparatos terminales han estado sometidos potencialmente a un intento de manipulación y llevan estos aparatos terminales por ejemplo a un estado seguro. Esto se realiza por ejemplo mientras un aparato terminal afectado comunica aún con el back-end o en la siguiente comunicación de un aparato terminal afectado con el back-end.

En otras formas de realización del procedimiento cumple el canal de comunicación seguro exigencias de seguridad, que son fijadas por el back-end, comprobando el aparato terminal en particular la primera firma digital, para determinar si el canal de comunicación realmente cumple las exigencias de seguridad del back-end.

Con ello puede determinar el back-end por ejemplo parámetros de seguridad, como fortaleza de la clave o el protocolo de comunicación y puede fijar así implícitamente también la información de enlace del canal. Esto tiene la ventaja de que el back-end puede fijar las exigencias de seguridad para la comunicación con el aparato terminal, sin que el aparato terminal tenga que disponer de funciones criptográficas o bien protocolos de comunicación criptográficos.

Según otro aspecto, se refiere la invención a un sistema. El sistema presenta un back-end, un interlocutor de comunicación y un aparato terminal. Además incluye el back-end un primer equipo de criptografía, un primer equipo de comunicación y un equipo de generación. El equipo de generación confecciona una estructura de datos y una primera firma digital sobre la estructura de los datos mediante el primer equipo de criptografía y una primera clave privada, pudiendo comprobarse la primera firma digital con una primera clave pública. El primer equipo de comunicación está programado mediante un primer procesador para enviar la estructura de los datos y la firma digital a un aparato terminal. Adicionalmente está programado el primer equipo de comunicación mediante el primer procesador para establecer un canal de comunicación seguro con un interlocutor de comunicación mediante un protocolo de comunicación utilizando el primer equipo de criptografía, determinándose en cada caso una información de enlace del canal mediante el protocolo de comunicación para el back-end y para el interlocutor de comunicación. El interlocutor de comunicación incluye un segundo equipo de criptografía y un segundo equipo de comunicación. El segundo equipo de comunicación está programado mediante un segundo procesador para establecer el canal de comunicación seguro con el back-end utilizando el segundo equipo de criptografía. Adicionalmente está programado el segundo equipo de comunicación mediante el segundo procesador para establecer un canal de comunicación con el aparato terminal. Adicionalmente está programado el segundo equipo de comunicación mediante el segundo procesador para enviar informaciones de enlace del canal al aparato terminal. El aparato terminal incluye un tercer equipo de comunicación, un equipo de prueba y una memoria. El tercer equipo de comunicación está programado mediante un tercer procesador para establecer el canal de comunicación con el interlocutor de comunicación. Adicionalmente está programado el tercer equipo de comunicación mediante el tercer procesador para recibir las informaciones de enlace del canal y/o la estructura de datos y/o la primera firma digital y/o la primera clave pública. El equipo de prueba comprueba la autenticidad de la estructura de datos mediante un algoritmo de prueba utilizando la primera firma digital y la primera clave pública. La memoria memoriza las informaciones de enlace del canal y/o la estructura de datos y/o la primera firma digital y/o la primera clave pública.

En una primera forma de realización del sistema, el sistema es un sistema virtualizado total o parcialmente.

De esta manera se pueden implementar en particular componentes del sistema favorablemente, sin utilizar un costoso hardware.

Además se utiliza un producto de programa de computadora con órdenes de programa para realizar el procedimiento de acuerdo con la invención antes citado. Adicionalmente se utiliza un dispositivo de aportación para memorizar y/o proporcionar una estructura de datos que incluye el producto de programa de ordenador. El dispositivo de aportación es por ejemplo un soporte de datos, que almacena o proporciona el producto de programa de computadora. Alternativamente el sistema de aportación es por ejemplo un sistema de computadora, un sistema servidor, una red, un sistema de computadora basado en nube (cloud) y/o sistema de ordenador virtual que almacena y/o proporciona el producto de programa de computadora. Esta aportación se realiza con preferencia como descarga (download) del producto de programa de computadora completo, pero puede también por ejemplo realizarse como descarga parcial, que está compuesta por varias partes y que en particular se descarga a través de una red peer-to-peer (entre iguales). Un tal producto de programa de computadora se lee por ejemplo utilizando el dispositivo de aportación en forma del soporte de datos en un sistema y ejecuta las órdenes del programa, con lo que el procedimiento de acuerdo con la invención se conduce sobre una computadora para realizarlo.

Las características, particularidades y ventajas de esta invención antes descritas, así como la forma como se alcanzan las mismas, se entenderán de forma más clara y explícita en relación con la siguiente descripción de los ejemplos de realización, que se describirán más en detalle en relación con las figuras. Al respecto muestran:

figura 1 una representación de un ejemplo de realización de un procedimiento para generar un canal de comunicación seguro para aparatos terminales y

figura 2 una representación de un ejemplo de realización de un sistema para generar un canal de comunicación seguro para aparatos terminales.

En las figuras se han dotado los elementos que tienen la misma función de las mismas referencias, siempre que no se indique otra cosa.

La figura 1 muestra una representación de un ejemplo de realización de un procedimiento para generar un canal de comunicación seguro para aparatos terminales 400, por ejemplo audífonos.

La calidad de las prestaciones de un audífono puede ajustarse por ejemplo mediante un llamado nivel de prestaciones (en inglés Performance Level). Es decir, cuanto más alto sea el nivel de prestaciones, tanto mejores son las prestaciones del audífono, pero también más alto es el precio del audífono. Si por ejemplo un audiólogo desea aumentar el nivel de prestaciones de un audífono para un cliente, entonces debe liberarse esta función en el audífono, por ejemplo mediante un ticket de licencia por parte del fabricante del audífono. El fabricante del audífono a su vez facturará el nivel de prestaciones más elevado al audiólogo y el audiólogo retransmitirá los costes más elevados correspondientemente a su cliente. El ticket de licencia antes mencionado corresponde entonces a una licencia para ajustar internamente el nivel de prestaciones de un audífono. Una herramienta de programación de un interlocutor de comunicación 300 asume entonces por un lado la comunicación con el aparato terminal 400 o bien audífono. Adicionalmente establece la herramienta de programación un canal de comunicación seguro con el back-end del fabricante del audífono con el que con preferencia mantiene el audiólogo una cuenta para pedidos y facturaciones y ha de autentificarse para ello con un nombre de usuario y una palabra de paso.

En detalle, se ejecuta en este ejemplo de realización en un aparato terminal 400, por ejemplo un audífono, mediante un interlocutor de comunicación 300, por ejemplo una workstation, con la herramienta de programación para el aparato terminal 400, una función deseada, por ejemplo un aumento del nivel de prestaciones del audífono. En otras palabras, desea el interlocutor de comunicación 300 liberar con la herramienta de programación la función deseada en el aparato terminal 400. Para ello debe por ejemplo el interlocutor de comunicación 300 solicitar una información de configuración, por ejemplo una licencia para liberar las funciones deseadas para el aparato terminal 400 en un back-end 200.

En una primera etapa del procedimiento 105 se establece un enlace seguro en forma de un canal de comunicación seguro o bien de seguridad protegida entre el interlocutor de comunicación 300 y el aparato terminal 200. Para ello se utiliza un protocolo de comunicación, por ejemplo un protocolo de encriptado híbrido como el protocolo de seguridad del transporte (en inglés TLS, Transport Layer Security Protocol). El protocolo de comunicación fija en cada caso informaciones de enlace del canal para un canal de comunicación asegurado entre el interlocutor de comunicación 300 y el back-end 200. Para la autentificación se ejecuta entonces por un lado una autentificación del back-end 200 por el lado del servidor, como parte del protocolo de comunicación y por otra parte se ejecuta una autentificación por parte de la herramienta de programación basándose en un nombre de usuario y en una palabra de paso del usuario de la herramienta de programación. El aparato terminal 400 no conoce este canal de comunicación asegurado y utiliza para la comunicación con la herramienta de programación o bien el interlocutor de comunicación 300 con preferencia un enlace no protegido criptográficamente o un enlace débilmente protegido criptográficamente como el enlace existente entre el interlocutor de comunicación 300 y el back-end 200.

Las informaciones de enlace del canal pueden entonces ser idénticas para el back-end 200 y para el interlocutor de comunicación 300. Alternativamente pueden utilizarse distintas informaciones de enlace del canal para el back-end 200 y para el interlocutor de comunicación 300. Entonces es necesario que a partir de una primera información de enlace del canal del interlocutor de comunicación 300 pueda calcularse una segunda información de enlace del canal del back-end 200 mediante una función de transformación. Pero también es posible que se calcule la primera información de enlace del canal a partir de la segunda información de enlace del canal con la misma función de transformación u otra función de transformación adecuada. Adicionalmente debe conocer el aparato terminal 400 las funciones de transformación, para que el mismo pueda comprobar dado el caso una información de enlace del canal recibida en cuanto a si los datos recibidos del back-end 200 han sido solicitados a través del canal de comunicación seguro por el aparato terminal 400 o bien el interlocutor de comunicación 300. De esta manera pueden detectarse en particular manipulaciones en el canal de comunicación seguro.

Para que libere el interlocutor de comunicación 300 las funciones deseadas en el aparato terminal 400, se establece en una segunda etapa del procedimiento 110 un canal de comunicación desde el interlocutor de comunicación 300 al aparato terminal 400. La herramienta de programación puede ahora determinar para el canal de comunicación asegurado las informaciones de enlace del canal del interlocutor de comunicación 300.

Mediante la herramienta de programación se formula en una tercera etapa del procedimiento 115 una consulta al aparato terminal 400, para generar una nueva solicitud de licencia. Adicionalmente a la solicitud de licencia, contiene la consulta además las informaciones de enlace del canal del interlocutor de comunicación 300. El aparato terminal 400 memoriza en una etapa del procedimiento 120 este valor entonces hasta que se reciba el nuevo ticket de licencia.

El aparato terminal 400 genera mediante un generador de aleatoriedad funciones de seguridad, por ejemplo en forma de un número aleatorio, que también se denomina nonce (en inglés number used once) y envía en una cuarta etapa del procedimiento 121 estas informaciones de seguridad a la herramienta de programación, junto con una información de identidad, por ejemplo un identificador de aparato inequívoco, del aparato terminal 400. Para liberar las funciones deseadas, envía el aparato terminal 400 adicionalmente una solicitud de licencia al interlocutor de comunicación 300 o bien a la herramienta de programación. Estas informaciones del aparato terminal, es decir, la solicitud de licencia, las informaciones de seguridad y la información de identidad, se transmiten juntas en una quinta etapa del procedimiento 122 con informaciones adicionales del interlocutor de comunicación 300, por ejemplo informaciones de usuario relativas al usuario actual de la herramienta de programación, al back-end 200.

El back-end 200 a su vez comprueba la autorización y confecciona en una sexta etapa del procedimiento 125 una estructura de datos, por ejemplo un ticket de licencia, con el nuevo valor de licencia solicitado para las funciones deseadas que han de liberarse. El ticket de licencia está compuesto por ejemplo por la solicitud de licencia, la información de enlace del canal correspondiente al back-end 200 y la primera firma digital sobre la información de identidad, el nonce y un nuevo valor de licencia. El back-end 200 posee para ello la primera clave privada necesaria para la generación de la firma y el aparato terminal 400 la correspondiente primera clave pública, que es necesaria para comprobar la primera firma digital. La primera clave pública debe protegerse en el aparato terminal 400 solamente frente a modificación. También puede decirse que el aparato terminal 400 posee el certificado raíz (Root) de la primera clave pública del back-end 200.

En una séptima etapa del procedimiento 130 envía el back-end 200 la estructura de datos y la primera firma digital al aparato terminal 400. Estos datos, es decir, la primera firma digital y la estructura de datos, pueden enviarse por ejemplo a través de un canal separado no protegido criptográficamente al aparato terminal 400. Pero alternativamente puede utilizarse también el enlace existente mediante el interlocutor de comunicación 300 para el envío.

Con ello no sólo tiene el aparato terminal 400 la posibilidad de comprobar en una octava etapa del procedimiento 135 mediante un algoritmo de pruebas que el ticket de licencia es correcto criptográficamente, sino también si el ticket de licencia se ha proporcionado a través del canal de comunicación asegurado, que responde a las exigencias de seguridad (en inglés Security Policy), por ejemplo la fortaleza del procedimiento criptográfico, la fortaleza de la autentificación, la protección de la integridad y también el encriptado del back-end 200. Esto se determina prescribiendo el back-end 200 las exigencias de seguridad para el canal de comunicación asegurado hacia el interlocutor de comunicación 300. Puesto que el aparato terminal 400 comprueba mediante el algoritmo de prueba si hay suficiente coincidencia de las informaciones de enlace del canal memorizadas en el aparato terminal 400 y las informaciones de enlace del canal de la estructura de datos o bien de la primera firma digital, puede asegurarse así que se cumplen las exigencias de seguridad del back-end 200 indirectamente en el aparato terminal 400. Para ello es condición necesaria una relación de confianza del aparato terminal 400 respecto al back-end 200, que resulta en base al certificado raíz existente en el aparato terminal 400.

En una novena etapa del procedimiento 140, proporciona el aparato terminal 400 y/o el interlocutor de comunicación 300 por ejemplo una señal, que incluye una información de control, cuando el algoritmo de prueba detecta una autenticidad no válida para la primera firma digital o una coincidencia insuficiente de las informaciones de enlace del canal memorizadas en el aparato terminal 400 y las informaciones de enlace del canal enviadas por el back-end.

En una variante, se realiza mediante el protocolo de comunicación, en lugar de una autentificación unilateral entre el back-end 200 y el interlocutor de comunicación 300, una autentificación mutua mediante un procedimiento de Handshake (relación de confianza), por ejemplo un Handshake TLS, basándose en certificados digitales, por ejemplo certificados X.509 y las correspondientes claves privadas. Al respecto, puede encontrarse idealmente la información de usuario en el certificado del interlocutor de comunicación 300. Con ello puede renunciarse dado el caso a la autentificación mediante un nombre de usuario y una palabra de paso.

En otra variante se utiliza para la comunicación entre el interlocutor de comunicación 300 o bien la herramienta de programación y el aparato terminal 400 un protocolo con una protección de la comunicación integrada. No obstante, esto presupone por ambos lados el correspondiente material de claves, por ejemplo un segundo par de claves con una segunda clave privada y una segunda clave pública. Un protocolo posible es a su vez el protocolo TLS. Por supuesto las exigencias de seguridad son aquí preferiblemente más débiles que las exigencias de seguridad al canal de comunicación seguro.

En otra variante más, se forman las informaciones de enlace del canal mediante uno de los siguientes parámetros. Pero también es posible formar la información de enlace del canal a partir de varios parámetros.

- Un identificador para el canal de comunicación seguro o la sesión entre el back-end 200 y el interlocutor de comunicación 300. Por ejemplo puede utilizarse, cuando se utiliza el protocolo TLS, el parámetro tlsunique.
- Un identificador del emisor del canal de comunicación asegurado.
- Un identificador del receptor del canal de comunicación asegurado.
- Informaciones relativas a la seguridad negociada para la comunicación, por ejemplo el procedimiento de autentificación utilizado, la protección de integridad utilizada y/o el nivel de confidencialidad utilizado.
- Un sello de tiempo, por ejemplo el instante en el que se generó el canal de comunicación asegurado.
- Un nonce, que por ejemplo fue generado por un generador de aleatoriedad.
-

En otra variante más, comprueba el interlocutor de comunicación o bien la herramienta de programación el ticket de licencia antes de que se retransmita al aparato terminal 400. Esto es especialmente procedente cuando el aparato terminal 400 está limitado en cuanto a memoria y/o capacidad de cálculo. Entonces dependen posibles reacciones, por ejemplo el borrado de datos, el procesamiento de un aviso de falta, la generación de una alarma, de la herramienta de programación, del comportamiento en cuanto a confidencialidad entre los abonados, es decir, el back-end 200, el interlocutor de comunicación 300 y el aparato terminal 400.

El sistema de computadora 500 incluye un back-end 200, por ejemplo en forma de un servidor de licencias de un fabricante de audífonos, con preferencia un servidor con un sistema operativo Linux. El servidor de licencias está por ejemplo conectado con una primera interfaz 225 a través de una conexión de Internet 505 con una segunda interfaz 320 de un interlocutor de comunicación 300 en forma de una computadora de un audiólogo, preferentemente un Apple iMac. El interlocutor de comunicación 300 está conectado por ejemplo mediante la segunda interfaz 320, a través de un enlace de red local 510, preferiblemente un enlace de red inalámbrico, con la tercera interfaz 425 de un aparato terminal 400, con preferencia un audífono.

El back-end 200 y el interlocutor de comunicación 300 incluyen por ejemplo respectivos componentes de hardware usuales en el mercado, como un aparato indicador óptico, preferiblemente en forma de un monitor TFT, al menos un aparato de entrada con preferencia en forma de un ratón de computadora y/o un teclado, al menos un soporte de datos, con preferencia en forma de un disco duro de estado sólido (solid-state) y/o de un reproductor de DVD de lectura y/o escritura, un procesador, con preferencia un procesador Intel x86 compatible, una interfaz de red, con preferencia una interfaz Ethernet, memoria de trabajo, con preferencia DDR RAM y/u otros hardware o aparatos periféricos conocidos por el especialista.

Adicionalmente incluye el back-end 200 un primer equipo de criptografía 205, un equipo de generación 210, un primer equipo de comunicación 215 y la primera interfaz 225, que están conectados entre sí comunicativamente a través de un primer bus interno 220, por ejemplo un bus de datos. El equipo de generación 210 crea una estructura de datos y una primera firma digital a través de la estructura de datos mediante el primer equipo de criptografía 205 y una primera clave privada, pudiendo comprobarse la primera firma digital con una primera clave pública. El primer equipo de comunicación 215 está programado mediante un primer procesador para enviar la estructura de datos y la primera firma digital a un aparato terminal 400. Adicionalmente está programado el primer equipo de comunicación 215 mediante el primer procesador para establecer un canal de comunicación seguro con un interlocutor de comunicación 300 mediante un protocolo de comunicación utilizando el primer equipo de criptografía 205, determinándose en cada caso una información de enlace del canal mediante el protocolo de comunicación para el back-end 200 y para el interlocutor de comunicación 300.

Adicionalmente incluye el interlocutor de comunicación 300 un segundo equipo de criptografía 305, un segundo equipo de comunicación 310 y la segunda interfaz 320, que están conectados entre sí comunicativamente a través de un segundo bus interno 315, por ejemplo un bus de datos. El segundo equipo de comunicación 310 está programado mediante un segundo procesador para establecer el canal de comunicación seguro con el back-end 200 utilizando el segundo equipo de criptografía 305. Adicionalmente está programado el segundo equipo de comunicación 310 mediante el segundo procesador para establecer un canal de comunicación con el aparato terminal 400. Adicionalmente está programado el segundo equipo de comunicación 310 mediante el segundo procesador para enviar las informaciones de enlace del canal al aparato terminal 400.

El aparato terminal 400 incluye un tercer equipo de comunicación 405, un equipo de prueba 410, una memoria 415 y la tercera interfaz 425, que están conectados comunicativamente entre sí a través de un tercer bus interno 420, por ejemplo un bus de datos. Además presenta el aparato terminal 400 otros componentes conocidos por el especialista, que se conocen por el estado de la técnica para un audífono.

El tercer equipo de comunicación 405 está programado mediante un tercer procesador para establecer el canal de comunicación con el interlocutor de comunicación 300. Adicionalmente está programado el tercer

equipo de comunicación 405 mediante el tercer procesador para recibir las informaciones de enlace del canal y/o la estructura de datos y/o la primera firma digital y/o la primera clave pública.

El equipo de prueba 410 comprueba la autenticidad de la estructura de datos mediante un algoritmo de prueba utilizando la primera firma digital y la primera clave pública.

La memoria 415 memoriza las informaciones de enlace del canal y/o la estructura de datos y/o la primera firma digital y/o la primera clave pública.

Aún cuando la invención se ha ilustrado y descrito en detalle mediante los ejemplos de realización, la invención no queda limitada por los ejemplos dados a conocer y el especialista puede deducir de aquí otras variaciones sin abandonar el ámbito de protección de la invención.

REIVINDICACIONES

1. Procedimiento (100) para generar un canal de comunicación seguro para un aparato terminal (400), incluyendo el procedimiento las siguientes etapas del procedimiento
   - establecimiento (105) de un canal de comunicación seguro mediante un protocolo de comunicación entre un interlocutor de comunicación (300) y un back-end (200), determinándose en cada caso una información de enlace del canal para el back-end (200) y para el interlocutor de comunicación (300) mediante el protocolo de comunicación;
   - generación (110) de un canal de comunicación entre el interlocutor de comunicación (300) y el aparato terminal (400);
   - transmisión (115) de la información de enlace del canal relativa al canal de comunicación seguro por medio del interlocutor de comunicación (300) al aparato terminal (400);
   - memorización (120) de la información de enlace del canal en el aparato terminal (400);
   - confección (125) de una estructura de datos y una primera firma digital mediante la estructura de datos por medio del back-end (200) con una primera clave privada, pudiendo comprobarse la firma digital con una primera clave pública;
   - envío (130) de la estructura de datos y de la firma digital desde el back-end (200) al aparato terminal (400) y
   - comprobación (135) de una autenticidad de la estructura de datos mediante un algoritmo de prueba para verificar la firma digital mediante la clave pública por parte del aparato terminal (400) y/o por parte del interlocutor de comunicación (300),

   caracterizado porque
   - la estructura de datos incluye la información de enlace del canal y/o informaciones básicas del back-end (400),
   - el algoritmo de prueba, para detectar la autenticidad, comprueba adicionalmente la información de enlace del canal memorizada y la información de enlace del canal,
   - el canal de comunicación seguro cumple exigencias de seguridad, que son fijadas por el back-end (200), comprobando el aparato terminal (400) la primera firma, para determinar si el canal de comunicación realmente cumple las exigencias de seguridad del back-end (200)

2. Procedimiento (100) de acuerdo con la reivindicación 1,
   presentando el procedimiento una etapa del procedimiento adicional para enviar informaciones de seguridad y/o informaciones de identidad desde el aparato terminal (400) a través del interlocutor de comunicación (300) al back-end (200).

3. Procedimiento (100) de acuerdo con la reivindicación 1,
   presentando el procedimiento las siguientes etapas del procedimiento:
   - envío (121) de las informaciones de seguridad e informaciones de identidad del aparato terminal (400) desde el aparato terminal (400) al interlocutor de comunicación (300);
   - envío (122) de las informaciones de seguridad e informaciones de identidad del aparato terminal (400) desde el interlocutor de comunicación (300) a través del canal de comunicación seguro al back-end (200).

4. Procedimiento (100) de acuerdo con una de las reivindicaciones precedentes,
   en el que se proporciona una señal a través del aparato terminal (400) y/o a través del interlocutor de comunicación (300), cuando el algoritmo de prueba detecta una autenticidad no válida.

5. Procedimiento (100) de acuerdo con una de las reivindicaciones precedentes,
   en el que se proporciona la primera clave pública para el aparato terminal (400), proporcionando una entidad certificadora o el back-end (200) la primera clave pública.

6. Procedimiento (100) de acuerdo con una de las reivindicaciones 3 a 5,
   en el que las informaciones de base del back-end (200) incluyen una información de configuración, incluyendo la información de configuración una información de licencia y/o código de programa para ejecutar una orden, que lleva a cabo el aparato terminal (400) sobre el aparato terminal (400).

7. Procedimiento (100) de acuerdo con una de las reivindicaciones 2 a 6,
   en el que el aparato terminal (400) dispone de un segundo par de claves en forma de una segunda clave pública y una segunda clave privada, con la que se genera para las informaciones de seguridad del aparato terminal (400) una segunda firma digital.

8. Procedimiento (100) de acuerdo con la reivindicación 7,
   en el que el interlocutor de comunicación (300) comprueba una segunda autenticidad de la información de seguridad mediante la segunda clave pública.

9. Procedimiento (100) de acuerdo con una de las reivindicaciones 2 a 8,
   en el que la información de seguridad presenta un nonce y/o un identificador de un certificado del aparato terminal y/o sólo una huella digital de la segunda clave pública.

10. Procedimiento (100) de acuerdo con una de las reivindicaciones 2 a 8,
en el que la información de seguridad y/o la información de enlace del canal y/o las informaciones de identidad se incluyen, total o parcialmente, en la primera firma digital.

11. Procedimiento (100) de acuerdo con una de las reivindicaciones precedentes,
en el que la estructura de datos y/o la primera firma digital incluyen una información de legitimidad, que da lugar a que el aparato terminal (400) conecte una determinada programación.

12. Procedimiento (100) de acuerdo con una de las reivindicaciones precedentes,
en el que la estructura de datos se amplía en la primera firma digital.

13. Procedimiento (100) de acuerdo con una de las reivindicaciones 2 a 12,
en el que la estructura de datos incluye adicionalmente las informaciones de seguridad y/o informaciones de identidad del aparato terminal (400)

14. Procedimiento (100) de acuerdo con una de las reivindicaciones precedentes,
en el que el algoritmo de prueba se ejecuta en el aparato terminal (400) y/o en el interlocutor de comunicación (300).

15. Procedimiento (100) de acuerdo con una de las reivindicaciones 2 a 14,
en el que al enviar las informaciones de seguridad e informaciones de identidad desde el interlocutor de comunicación (300) al back-end (400), el interlocutor de comunicación (300) envía a la vez informaciones adicionales, incluyendo las informaciones adicionales una información de usuario.

16. Procedimiento (100) de acuerdo con una de las reivindicaciones precedentes,
en el que la primera clave pública se envía a la vez cuando se envía la estructura de datos.

17. Procedimiento (100) de acuerdo con una de las reivindicaciones 1 a 15,
en el que la clave pública se proporciona en un instante más temprano al aparato terminal (400), siendo el instante más temprano el momento de la fabricación del aparato terminal (400).

18. Procedimiento (100) de acuerdo con una de las reivindicaciones precedentes,
en el que la clave pública está protegida contra una modificación en el aparato terminal (400)

19. Procedimiento (100) de acuerdo con una de las reivindicaciones precedentes,
en el que la primera clave privada es un secreto que el back-end (200) conoce, siendo conocido el secreto exclusivamente por el back-end (200).

20. Procedimiento (100) de acuerdo con una de las reivindicaciones precedentes,
en el que el aparato terminal (400) sólo dispone de informaciones no críticas para la seguridad.

21. Procedimiento (100) de acuerdo con una de las reivindicaciones precedentes,
en el que el canal de comunicación seguro se genera mediante un procedimiento simétrico, o el canal de comunicación seguro se genera mediante un procedimiento asimétrico, utilizando el procedimiento asimétrico un certificado digital.

22. Procedimiento (100) de acuerdo con una de las reivindicaciones 4 a 21,
en el que la señal es evaluada por el back-end (200) u otro interlocutor de comunicación.

23. Procedimiento (100) de acuerdo con una de las reivindicaciones precedentes,
en el que el interlocutor de comunicación comprueba la primera clave pública antes de retransmitir la primera clave pública al aparato terminal, siendo la clave pública un certificado, validándose el certificado frente a un expedidor conocido, incluyendo la validación del certificado una validez y/o un estado de rechazo.

24. Back-end (200) que presenta
- un primer equipo de criptografía (205),
- un equipo de generación (210) para confeccionar una estructura de datos y una primera firma digital sobre la estructura de los datos mediante el primer equipo de criptografía (205) y una primera clave privada, pudiendo comprobarse la primera firma digital con una primera clave pública;
- un primer equipo de comunicación (215) que está programado mediante un primer procesador
  - para enviar la estructura de los datos y la primera firma digital a un aparato terminal (400);
  - para establecer un canal de comunicación seguro con un interlocutor de comunicación (300) mediante un protocolo de comunicación utilizando el primer equipo de criptografía (205), determinándose en cada caso una información de enlace del canal mediante el protocolo de comunicación para el back-end (200) y para el interlocutor de comunicación (300)

caracterizado porque

- la estructura de datos incluye la información de enlace del canal y/o informaciones básicas del back-end (400),
- el canal de comunicación seguro cumple exigencias de seguridad, que son fijadas por el back-end (200), comprobando el aparato terminal (400) la primera firma, para determinar si el canal de comunicación realmente cumple las exigencias de seguridad del back-end (200).

25. Interlocutor de comunicación (300) que presenta

- un segundo equipo de criptografía (305);
- un segundo equipo de comunicación (310), que está programado mediante un segundo procesador
  - para establecer un canal de comunicación seguro con un back-end (200) utilizando el segundo equipo de criptografía (305), fijándose en cada caso una información de enlace del canal mediante el protocolo de comunicación para el back-end (200) y para el interlocutor de comunicación (300),
  - para establecer un canal de comunicación con un aparato terminal (400) y
  - para enviar informaciones de enlace del canal al aparato terminal (400)

caracterizado porque

- una estructura de datos del back-end (400) incluye la información de enlace del canal y/o informaciones de base del back-end (400),
- el canal de comunicación seguro cumple exigencias de seguridad, que son fijadas por el back-end (200), comprobando el aparato terminal (400) una primera firma generada por el back-end (200) sobre la estructura de datos, para determinar si el canal de comunicación realmente cumple las exigencias de seguridad del back-end (200).

26. Aparato terminal (400) que presenta

- un tercer equipo de comunicación (405), que está programado mediante un tercer procesador
  - para establecer un canal de comunicación con un interlocutor de comunicación (300),
  - para recibir las informaciones de enlace del canal y/o una estructura de datos y/o una primera firma digital y/o una clave pública, habiéndose generado la primera firma digital mediante la estructura de datos por parte del back-end (200) con una primera clave privada;
- un equipo de prueba (410) para comprobar una autenticidad de la estructura de datos mediante un algoritmo de prueba utilizando la primera firma digital y la clave pública;
- una memoria (415) para memorizar las informaciones de enlace del canal y/o la estructura de datos y/o la primera firma digital y/o la primera clave pública,

caracterizado porque

- la estructura de datos incluye la información de enlace del canal y/o informaciones básicas del back-end (400),
- el algoritmo de prueba, para detectar la autenticidad, comprueba adicionalmente la información de enlace del canal memorizada y la información de enlace del canal,
- el canal de comunicación seguro cumple exigencias de seguridad, que son fijadas por el back-end (200), comprobando el aparato terminal (400) la primera firma, para determinar si el canal de comunicación realmente cumple las exigencias de seguridad del back-end (200).

27. Sistema (500)

que presenta

- un Back-end (200) con
- un primer equipo de criptografía (205);
- un equipo de generación (210) para confeccionar una estructura de datos y una primera firma digital sobre la estructura de datos mediante el primer equipo de criptografía (205) y una primera clave privada, pudiendo comprobarse la primera firma digital con una primera clave pública;
- un primer equipo de comunicación (215) que está programado mediante un primer procesador
  - para enviar la estructura de los datos y la primera firma digital a un aparato terminal (400);
  - para establecer un canal de comunicación seguro con un interlocutor de comunicación (300) mediante un protocolo de comunicación utilizando el primer equipo de criptografía (205), determinándose en cada caso una información de enlace del canal mediante el protocolo de comunicación para el back-end (200) y para el interlocutor de comunicación (300);
- el interlocutor de comunicación (300) con
  - un segundo equipo de criptografía (305);
  - un segundo equipo de comunicación (310), que está programado mediante un segundo procesador
    - para establecer el canal de comunicación seguro con el back-end (200) utilizando el segundo equipo de criptografía (305),
    - para establecer un canal de comunicación con el aparato terminal (400) y
    - para enviar las informaciones de enlace del canal al aparato terminal (400);
- el aparato terminal (400) con

- un tercer equipo de comunicación (405), que está programado mediante un tercer procesador
  - para establecer el canal de comunicación con un interlocutor de comunicación (300),
  - para recibir las informaciones de enlace del canal y/o la estructura de datos y/o la primera firma digital y/o la clave pública,
- un equipo de prueba (410) para comprobar una autenticidad de la estructura de datos mediante un algoritmo de prueba utilizando la primera firma digital y la clave pública;
- una memoria (415) para memorizar las informaciones de enlace del canal y/o la estructura de datos y/o la primera firma digital y/o la primera clave pública,

caracterizado porque

- la estructura de datos incluye la información de enlace del canal y/o informaciones básicas del back-end (400),
- el algoritmo de prueba, para detectar la autenticidad, comprueba adicionalmente la información de enlace del canal memorizada y la información de enlace del canal,
- el canal de comunicación seguro cumple exigencias de seguridad, que son fijadas por el back-end (200), comprobando el aparato terminal (400) la primera firma, para determinar si el canal de comunicación realmente cumple las exigencias de seguridad del back-end (200).

28. Sistema (500) de acuerdo con la reivindicación 27, siendo el sistema un sistema virtualizado.

29. Producto de programa de computadora con órdenes de programa, que cuando las órdenes son ejecutadas por una computadora, hacen que la computadora ejecute todas las etapas del procedimiento correspondientes al procedimiento de acuerdo con una de las reivindicaciones 1- 23.

30. Dispositivo de aportación para el producto de programa de ordenador de acuerdo con la reivindicación 29, memorizando y/o aportando el dispositivo de aportación el producto de programa de computadora.

FIG 1

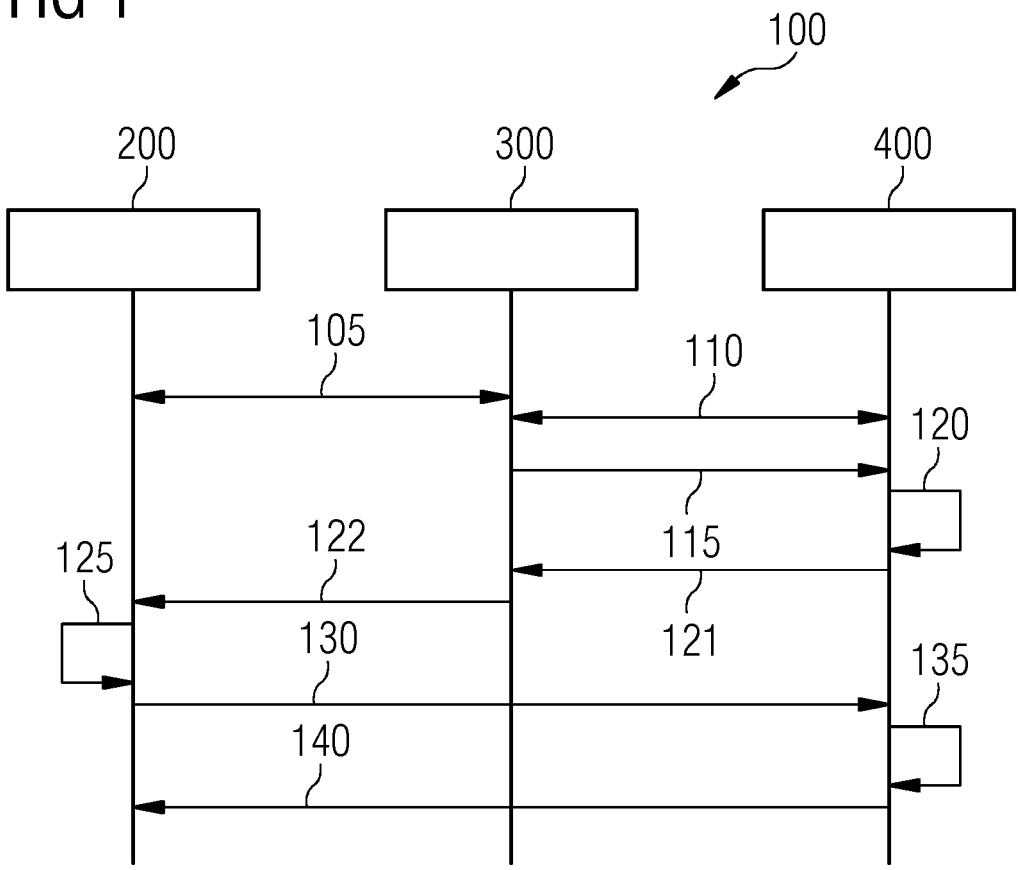
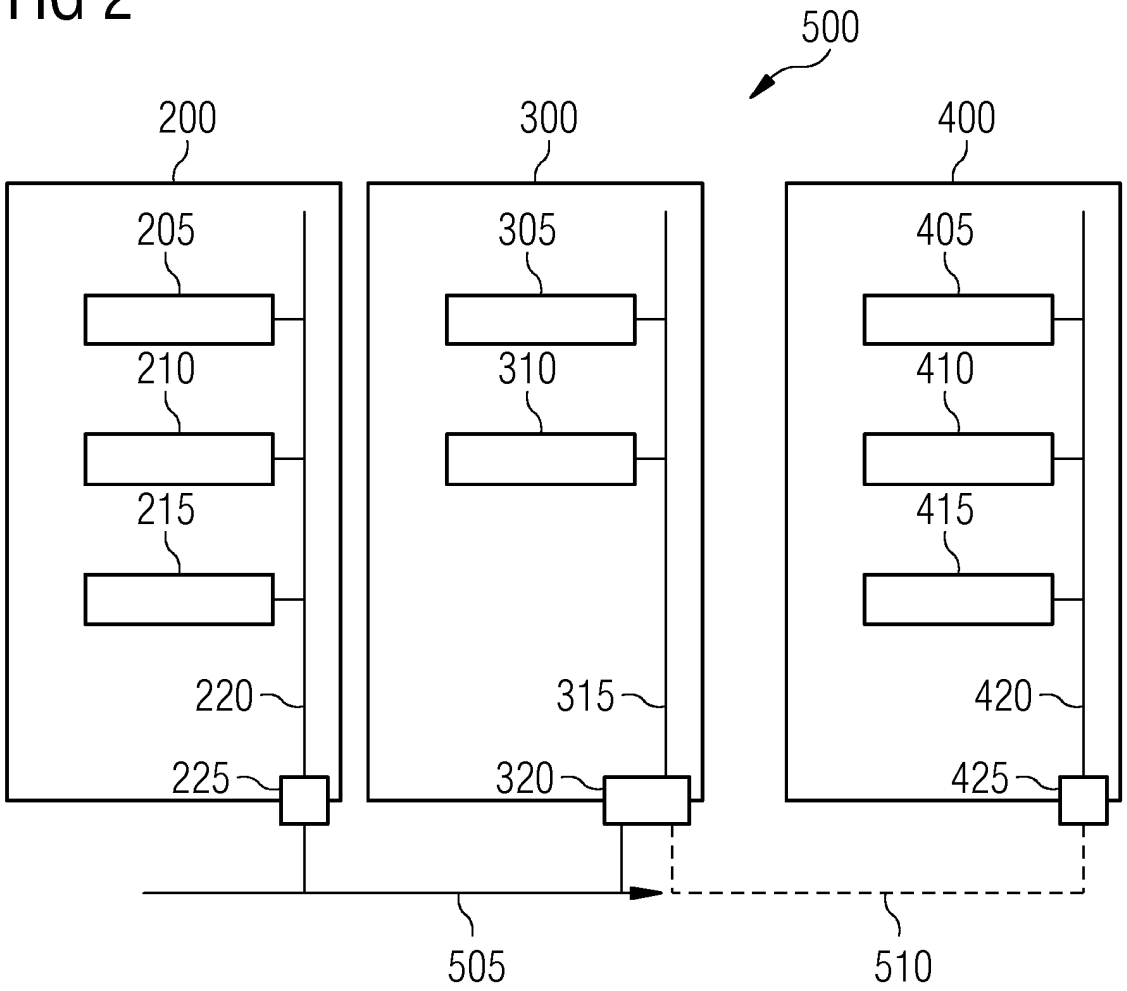


FIG 2


500
200
300
400
205
305
405
210
310
410
215
415
220
315
420
225
320
425
505
510