(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 434 335**

(51) Int. CI.:

G06F 21/00 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.07.2006 E 06116828 (2)**

(97) Fecha y número de publicación de la concesión europea: **14.08.2013 EP 1876550**

(54) Título: **Procedimiento y sistema para la transmisión de datos encriptada**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.12.2013

(73) Titular/es:

SWISSCOM AG (100.0%)
ALTE TIEFENAUSTRASSE 6
WORBLAUFEN/ITTIGEN
3050 BERN, CH

(72) Inventor/es:

LINDER, JAN;
DANZEISEN, MARC;
WINIKER, SIMON y
BAUMGARTNER, FLORIAN

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

PROCEDIMIENTO Y SISTEMA PARA LA TRANSMISION DE DATOS ENCRIPTADA

Ambito técnico

La presente invención se refiere a un procedimiento y un sistema para la transmisión de datos.

Estado de la técnica

Una transmisión de datos entre terminales y/o servidores se realiza, según el estado de la técnica, de acuerdo con diversos procedimientos. A menudo tales procedimientos están particularmente adaptados para transmitir noticias, tales como por ejemplo noticias de e-mail o titulares de actualidad, o para transmitir datos de multimedia, tales como un fichero de audio o un fichero de vídeo. Para transmitir por ejemplo datos desde un servidor a un terminal de un usuario puede resultar necesario que primeramente sea comprobada la autorización del usuario para el acceso a determinados datos. Una tal comprobación de la autorización puede por ejemplo efectuarse mediante la consulta de un nombre de usuario y de una contraseña. Dado que una transmisión de datos se efectúa frecuentemente a través de redes públicas, resulta ventajoso realizar dicha transmisión de datos mediante una conexión de datos asegurada, tal como por ejemplo mediante una conexión VPN (VPN: Virtual Private Network). De esta manera puede subdividirse la transmisión de datos entre un servidor y un terminal en una fase de comprobación de la autorización o una fase de autentificación y una fase de transmisión de datos. Debido a

la interacción con el usuario la fase de autentificación es a menudo de relativamente larga duración, aunque solamente se precisa poco ancho de banda de red. La fase de transmisión de datos, por el contrario, puede durar, según el volumen de datos, solamente poco tiempo, mientras que se aprovecha plenamente el ancho de banda de red disponible.

Así por ejemplo, noticias de e-mail para un usuario son almacenadas en un servidor de e-mail. El usuario baja las noticias de e-mail almacenadas en el servidor de e-mail mediante un cliente de e-mail. Para ello se emplean, en el estado de la técnica, protocolos tales como POP (POP: Post Office Protocol) o IMAP (IMAP: Internet Mail Access Protocol). Mediante el cliente de e-mail y tales protocolos se constituye entre el cliente de e-mail y el servidor de e-mail una comunicación, tras lo cual el cliente de e-mail comprueba el servidor de e-mail en cuanto a noticias de e-mail disponibles y eventualmente descarga nuevas noticias de e-mail al cliente de e-mail. Naturalmente es comprobado el cliente de e-mail mediante una autentificación en cuanto a la autorización para el acceso a las noticias de e-mail. A menudo dura la autentificación mucho más que la subsiguiente comprobación y descarga de las noticias de e-mail. La comprobación de noticias de e-mail puede también basarse en un VPN Tunnel. Sin embargo, en este caso se constituye un VPN Tunnel también aunque en el servidor de e-mail no esté disponible nueva noticia alguna. Ello da lugar a una ineficacia, ya que se constituye un VPN Tunnel incluso aunque no haya disponible dato alguno para la transmisión.

En el estado de la técnica una tal transmisión de datos en dos fases adolece de muchos inconvenientes, particularmente para usuarios de terminales móviles. Así por ejemplo, aunque el usuario dispone en estaciones de tren de potentes redes WLAN o UWB (WLAN: Wireless Local Area Network; UWB: Ultra Wide Band), a menudo no tiene tiempo para autentificarse para el acceso a datos y descargar datos al terminal móvil. Sin embargo, después de que el usuario se haya aposentado en el tren dispone frecuentemente de suficiente tiempo para autentificarse para el acceso a datos. Sin embargo, a menudo el tren ha abandonado entonces ya el recinto de la estación y el usuario dispone en este momento sólo de redes mucho menos potentes, tales como por ejemplo una red GSM o una red UMTS (GSM: Global System for Mobile Communications; UMTS: Universal Mobile Telecommunications System). Por consiguiente, el usuario no puede en ese momento acceder a grandes cantidades de datos, tal como por ejemplo a una noticia de e-mail con un fichero de vídeo adjunto, ya que la capacidad de transmisión de una tal red menos potente no bastaría. En resumen, la autentificación y subsiguiente transmisión de datos empleada en el estado de la técnica resulta, por una parte, inconveniente para el usuario, ya que éste precisa realizar una interacción de usuario. Por otra parte, este tipo de interacción de usuario da lugar a que se impida una optimización de la carga de una infraestructura de red.

En el documento EP 1 372 055 se divulga una arquitectura Digital Rights Management. Un Packager prepara datos para un usuario y un Licensor pone a disposición una licencia para el

usuario. El Packager y el Licensor comparten una llave secreta y pueden calcular una llave de contenido para los datos preparados. Los datos preparados y encriptados así como la llave de contenido son transmitidos al usuario.

Exposición de la invención

Constituye una finalidad de la presente invención proponer un nuevo procedimiento y un nuevo sistema para la transmisión de datos, cuyo procedimiento y cuyo sistema no adolezcan de los inconvenientes del estado de la técnica.

De acuerdo con la presente invención estas finalidades se consiguen particularmente mediante los elementos de las reivindicaciones independientes. Ulteriores formas de realización ventajosas se desprenden, además, de las reivindicaciones dependientes y de la descripción. Particularmente se consiguen estas finalidades, de acuerdo con la invención, mediante un procedimiento para la transmisión de datos, siendo ejecutado el procedimiento por un módulo central. El procedimiento comprende:

recepción de datos de autentificación de un aparato terminal de comunicación,

almacenamiento de los datos de autentificación, estando asociados los datos de autentificación a una identificación,

generación de una llave electrónica, almacenándose la llave electrónica de forma asociada a los datos de autentificación y a la identificación,

autentificación de una autorización en la llave electrónica para el aparato terminal de comunicación mediante los

datos de autentificación recibidos,

comprobación de una disponibilidad del aparato terminal de comunicación mediante un módulo de disponibilidad del módulo central,

generación de datos encriptados, mediante un módulo de encriptación, de datos y de al menos una parte de la llave electrónica,

transmisión de los datos encriptados y de al menos una parte de la llave electrónica al aparato terminal de comunicación, estando el aparato de comunicación disponible y autorizado.

Un tal procedimiento presenta particularmente la ventaja de que la transmisión de los datos de autentificación con respecto a la llave electrónica y la transmisión de los datos encriptados pueden efectuarse de manera totalmente asíncrona. Así pues pueden en el aparato terminal de comunicación crearse por ejemplo noticias de e-mail y encriptarse con la llave electrónica. En un momento cualquiera, por ejemplo tan pronto se halle el aparato terminal de comunicación en la zona de actuación de una red de comunicación inalámbrica, pueden transmitirse con seguridad los datos encriptados a través de la red de comunicación inalámbrica, ser descodificados por el módulo central y ser retransmitidos a un servidor de e-mail. Naturalmente pueden transmitirse datos encriptados tanto desde el módulo central al aparato terminal de comunicación como también desde el aparato terminal de comunicación al módulo central.

Un tal procedimiento presenta también la ventaja de que

la autentificación para el acceso a datos y la transmisión de datos propiamente dicha a un aparato terminal de comunicación pueden realizarse en instantes diversos. Así pues la transmisión de datos encriptados puede realizarse en un instante en que el usuario se halle en la proximidad de una red potente, y la autentificación para el acceso a la llave electrónica y por tanto a los datos puede realizarse en un instante en que el usuario tenga suficiente tiempo para realizar una autentificación.

De acuerdo con una variante de realización, en el módulo central o en el aparato terminal de comunicación, respectivamente, es almacenado un perfil de usuario, siendo seleccionados y encriptados datos de acuerdo con el perfil de usuario así como transmitidos al aparato terminal de comunicación o a un ulterior aparato de comunicación, respectivamente. Un tal procedimiento tiene particularmente la ventaja de que un usuario puede registrar en un perfil de usuario qué datos deben ser encriptados y transmitidos al aparato terminal de comunicación o al ulterior aparato de comunicación, respectivamente. Así por ejemplo puede estar registrado en un perfil de usuario que todas las noticias de e-mail de un usuario sean encriptadas y transmitidas al aparato terminal de comunicación del usuario siempre a una hora determinada, por ejemplo por la mañana cuando el usuario se halle en la estación para subir a un tren.

De acuerdo con la invención es comprobada mediante un módulo de disponibilidad del módulo central la disponibilidad del aparato terminal de comunicación y son transmitidos los

datos encriptados, en caso de disponibilidad del aparato terminal de comunicación, a dicho aparato terminal de comunicación. Un tal procedimiento presenta particularmente la ventaja de que los datos encriptados pueden ser transmitidos en el instante más pronto posible al aparato terminal de comunicación o al ulterior aparato de comunicación, respectivamente.

De acuerdo con una ulterior variante de realización es activado, mediante un módulo de activación del módulo central, un interfase de red del aparato terminal de comunicación y los datos encriptados son transmitidos, a través del interfase de red activado, al aparato terminal de comunicación. Así pues, por ejemplo un primer interfase de red del aparato terminal de comunicación, tal como por ejemplo un interfase de red GSM, puede estar constantemente conectado, y a través de este primer interfase de red puede activarse un segundo interfase de red, tal como por ejemplo un interfase de red WLAN, del aparato terminal de comunicación. Un tal procedimiento presenta particularmente la ventaja de que interfases de red son conectados por el módulo central únicamente cuando estén preparados datos encriptados para la transmisión, con lo que puede particularmente minimizarse el consumo de corriente en el aparato terminal de comunicación.

De acuerdo con otra variante de realización, los datos encriptados son transmitidos a un aparato de red de una infraestructura de red, siendo los datos encriptados almacenados en el aparato de red y transmitidos de forma asíncrona por el aparato de red al aparato terminal de comunicación. El mencionado aparato de red puede referirse por ejemplo a un

aparato de red de un WLAN Hotspot, siendo en un primer instante, por ejemplo en la mañana temprana a una hora con reducida carga de red, transmitidos los datos encriptados al aparato de red y en un segundo instante, por ejemplo cuando el usuario espere en la estación al tren, transmitidos de este aparato de red al aparato terminal de comunicación del usuario. Un tal procedimiento presenta particularmente la ventaja de que puede optimizarse la carga de una infraestructura de red. Naturalmente puede realizarse, antes de la encriptación de los datos, una adaptación de los datos a un aparato terminal de comunicación. Si por ejemplo el aparato terminal de comunicación del usuario se refiere a un ordenador móvil con una resolución de pantalla XGA de 1024 x 768 Pixel, no tiene sentido encriptar directamente un fichero de vídeo con una resolución muy elevada. En este caso resulta mucho más sensato adaptar el fichero de vídeo, mediante una transformación de la resolución, primeramente a la resolución de pantalla del usuario y únicamente luego realizar una encriptación del fichero de vídeo. Una tal transformación de los datos puede realizarse particularmente cuando por ejemplo estén almacenadas en un perfil de usuario correspondientes informaciones.

De acuerdo con otra variante de realización, durante la transmisión de la al menos una parte de la llave electrónica se carga un importe monetario en una cuenta de usuario. Un tal procedimiento posee particularmente la ventaja de que mediante la transmisión de datos encriptados pueden ofrecerse al usuario servicios de cargo, tales como por ejemplo la puesta a disposición de ficheros de audio o de vídeo. Natu-

ralmente, el servicio se considera como realizado únicamente cuando tanto los datos encriptados como también la correspondiente llave hayan sido transmitidos al aparato terminal de comunicación del usuario.

De acuerdo con una ulterior variante de realización, los datos encriptados comprenden un código de programa, cuyo código de programa debe ejecutarse para la descodificación de los datos encriptados, comprobándose durante la ejecución del código de programa criterios de validez. Así pues, el código de programa puede estar por ejemplo configurado de tal manera que la validez de la llave sea comprobada con respecto a una medición de tiempo, a un servidor central mediante el cual se vigile la validez de llaves o según cualquier otro procedimiento. Un tal procedimiento posee particularmente la ventaja de que puede por ejemplo definirse a partir de cuando los datos encriptados no estén ya disponibles. Mediante un tal procedimiento queda además garantizada la compatibilidad con procedimientos conocidos por el DRM (DRM: Digital Rights Management).

De acuerdo con una ulterior variante de realización, se asocia a los datos y/o a los datos encriptados una identificación y los datos de autentificación son almacenados de forma asociada a la identificación. Una tal identificación puede por ejemplo configurarse como resultado de una función Hash de los datos encriptados. Un tal procedimiento posee particularmente la ventaja de que la autentificación para el acceso a los datos encriptados puede configurarse diversamente también con respecto a los datos encriptados.

Breve descripción de los dibujos

A continuación se describirán variantes de realización de la presente invención mediante ejemplos. Los ejemplos de las formas de realización se ilustran en los dibujos adjuntos, en los cuales:

La Fig. 1 muestra un diagrama de bloques con los distintos componentes para la encriptación de datos y para la transmisión de los datos encriptados;

la Fig. 2 muestra un diagrama de bloques con los distintos componentes para la autentificación y descodificación de los datos encriptados; y

la Fig. 3 muestra un diagrama de bloques con los distintos componentes para la encriptación y para el envío de datos encriptados.

Vía(s) para la realización de la invención

En la Fig. 1 el número de referencia 10 se refiere a un módulo central. El módulo central 10 puede por ejemplo estar configurado a modo de módulo de software de un servidor de red. Naturalmente, el módulo central 10 puede también estar configurado totalmente como módulo de hardware con correspondientes circuitos electrónicos. En la Fig. 1 el signo de referencia D se refiere a datos electrónicos. Los datos D pueden ser cualquier tipo de datos electrónicos, por ejemplo noticias de e-mail, textos, animaciones, ficheros de audio, ficheros de vídeo o cualesquiera otros datos electrónicos. En la Fig. 1 el signo de referencia A se refiere a datos de autentificación y el signo de referencia S se refiere a una llave electrónica. Los datos de autentificación A pueden por

ejemplo comprender un nombre de usuario y una contraseña o una frase de paso. La llave electrónica S puede por ejemplo consistir de una llave electrónica simétrica con un secret key o de una llave electrónica asimétrica con un public key y un private key. Los datos de autentificación A son almacenados de forma asociada a la llave electrónica S, por ejemplo por el hecho de que el módulo central 10 comprenda una correspondiente tabla. En la Fig. 1 el número de referencia 40 se refiere a una red de comunicación. La red de comunicación puede por ejemplo referirse al Internet y puede estar constituida por varias redes de diversas tecnologías. Así pues, la red de comunicación puede comprender redes GSM, redes UMTS, redes WLAN, redes Ethernet, redes UWB o cualesquiera otras redes. Tal como se ilustra en la Fig. 1, el módulo central 10 es particularmente conectable con la red de comunicación 40. Mediante la llave electrónica S así como un módulo de encriptación del módulo central 10 pueden encriptarse datos D. Una tal encriptación puede referirse a cualquier algoritmo de encriptación, por ejemplo a un algoritmo DES (DES: Date Encryption Standard), a un algoritmo PGP (PGP: Pretty Good Privacy), a un algoritmo IDEA (IDEA: International Data Encryption Standard) o a cualquier otro algoritmo de encriptación. Mediante la encriptación de los datos D se generan datos encriptados vD. Los datos de autentificación A y la llave electrónica S pueden además almacenarse de forma asociada a una identificación iD de los datos, de manera que los datos de autentificación A y la llave electrónica S solamente sean válidos con respecto a datos que sean identificables por la

ción iD de los datos. Naturalmente pueden también preverse, con respecto a la identificación iD de los datos, correspondientes tablas en el módulo central 10.

En la Fig. 1 el número de referencia 20 se refiere a un aparato terminal de comunicación. El aparato terminal de comunicación 20 puede ser cualquier terminal de un usuario, por ejemplo un ordenador móvil tal como un portátil o un PDA (PDA: Personal Digital Assistant), un teléfono móvil, una consola de juego, un ordenador fijo o cualquier otro aparato terminal de comunicación. El aparato terminal de comunicación 20 es conectable, tal como se ilustra en la Fig. 1, con la red de comunicación 40. Una tal conexión puede referirse a una conexión inalámbrica, tal como por ejemplo una conexión WLAN, una conexión GSM o cualquier otra conexión inalámbrica, o a una conexión alámbrica, tal como por ejemplo una conexión Ethernet twisted-pair o cualquier otra conexión alámbrica.

De esta manera los datos encriptados vD pueden ser transmitidos, a través de la red de comunicación 40, al aparato terminal de comunicación 20 y ser allí almacenados. Existen las más diversas posibilidades para almacenar por tanto datos D como datos encriptados vD en el aparato terminal de comunicación 20. Así pues, en el aparato terminal de comunicación 20 pueden almacenarse noticias de e-mail, textos, animaciones, ficheros de audio, ficheros de vídeo o cualesquiera otros datos como noticias de e-mail encriptadas, textos encriptados, animaciones encriptadas, ficheros de audio encriptados o ficheros de vídeo encriptados. Sin embargo, ocurre que los datos encriptados vD pueden ser todavía inúti-

les, ya que la llave para la descodificación de los datos encriptados está de momento almacenada únicamente en el módulo central 10.

La transmisión de los datos encriptados vD al aparato terminal de comunicación 20 puede realizarse en cualquier instante oportuno. Así pues, un instante oportuno puede referirse a la llegada de nuevas noticias de e-mail, a la disponibilidad de textos o a la publicación de un nuevo fichero de audio. Sin embargo, un instante oportuno puede también referirse a la disponibilidad de una conexión de comunicación entre la red de comunicación 40 y el aparato terminal de comunicación 20, a la carga de la red de comunicación 40, a la carga de partes de la red de comunicación 40, a un instante que se produzca por una entrada del usuario en uno de los aparatos terminales de comunicación, o a cualquier otro instante.

La transmisión de los datos encriptados vD puede también producirse según distintos escenarios. Así pues, un escenario puede ser que los datos encriptados vD sean transmitidos en un instante cualquiera a través de una conexión de comunicación de banda ancha, tal como por ejemplo una conexión Ethernet, de noche al aparato terminal de comunicación 20. Un tal escenario puede por ejemplo elegirse para tansmitir un fichero de vídeo encriptado muy grande, tal como por ejemplo del orden de magnitud de 5 GByte, al aparato terminal de comunicación 20. O bien, en otro escenario, pueden transmitirse datos encriptados al aparato terminal de comunicación 20 tan pronto el usuario entre con este aparato terminal de comuni-

cación 20 en la zona de actuación de una red de comunicación inalámbrica, tal como por ejemplo una red WLAN o una red UWB en una estación o en el área de un aeropuerto. Un tal escenario puede por ejemplo elegirse para transmitir a un usuario, antes de subir al tren, noticias de e-mail encriptadas o textos encriptados a su aparato terminal de comunicación 20. Cabe mencionar aquí que textos encriptados pueden por ejemplo referirse a la edición diaria electrónica actual de un periódico.

En la Fig. 2 se mantienen los números de referencia introducidos en la Fig. 1. Tal como se ilustra en la Fig. 2, datos de autentificación A son transferidos desde el aparato terminal de comunicación 20 al módulo central 10. Con ello es autentificada la autorización en la llave electrónica S. A continuación son transmitidas al menos partes de la llave electrónica S desde el módulo central 10 al aparato terminal de comunicación 20. Mediante la llave electrónica S pueden descodificarse los datos encriptados vD almacenados en el aparato terminal de comunicación y almacenarse como datos D en el aparato terminal de comunicación, pudiendo el usuario acceder a estos datos D.

Una autentificación de la autorización en la llave electrónica S puede realizarse según procedimientos conocidos. Tales procedimientos pueden ejecutarse basados en contraseña, basados en frases de paso, mediante una tarjeta SecureID (SecureID: Procedimiento de autentificación de la firma RSA Security), basarse en la detección de características biométricas o basarse en cualquier otra prueba de autorización desea-

da.

Tal como se indica en las Figs. 1 a 3 mediante las zonas punteadas, la identificación iD, los datos de autentificación A y la llave S pueden estar almacenados en una tabla con duplas de tales datos. Concretamente, una determinada dupla puede estar prevista con una identificación iD, con datos de autentificación A y con una llave S para una determinada finalidad. Así pues, una primera dupla puede comprender una identificación iD que se refiera a datos de vídeo. Una segunda dupla puede comprender una identificación iD que se refiera a datos de audio. De esta manera pueden por ejemplo encriptarse datos de vídeo y datos de audio con una llave distinta, por ejemplo para datos de vídeo con una llave que dé lugar a una capacidad particularmente elevada en la descodificación de los datos de vídeo y por ejemplo para datos de audio con una llave que dé lugar a una seguridad particularmente elevada.

En la Fig. 2 el número de referencia 10' se refiere a una copia local del módulo central 10, aplicada al aparato terminal de comunicación 20. La copia local 10' del módulo central 10 puede comprender las mismas funcionalidades que el módulo central 10. Así pues, pueden almacenarse de las duplas con una identificación iD, con datos de autentificación A y con una llave S también copias locales en el aparato terminal de comunicación 20. La copia local 10' del módulo central así como las copias locales de las mencionadas duplas pueden por ejemplo protegerse mediante el empleo de una llave secreta, tal como por ejemplo un PIN (PIN: Personal Identification

Number). Así pues, puede estar previsto que el acceso a la copia local de estas funcionalidades y datos solamente resulte posible para un usuario que conozca la llave secreta. Naturalmente puede actualizarse esta copia local con funcionalidades y datos por ejemplo de manera incremental según las correspondientes funcionalidades y datos del módulo central 10. O bien pueden almacenarse en la copia local únicamente ciertas funcionalidades y datos.

Tal como se ilustra en la Fig. 3, en el aparato terminal de comunicación 20 pueden encriptarse datos D en datos encriptados vD y transmitirse a un ulterior aparato de comunicación. Así pues, en el aparato terminal de comunicación 20 puede estar almacenada una copia local 10' del módulo central 10 con la funcionalidad de la encriptación de datos y una correspondiente llave S. El usuario del aparato terminal de comunicación 20 puede por ejemplo captar de nuevo un fichero de vídeo. Tan pronto esté terminado el fichero de vídeo, este fichero de vídeo puede encriptarse, mediante las funcionalidades puestas a disposición por la copia local 10' del módulo central 10, en un fichero de vídeo encriptado. Naturalmente, el usuario también puede solicitar, mediante una correspondiente solicitud en el módulo central 10, una llave S para la encriptación del fichero de vídeo. El fichero de vídeo puede ser encriptado a un fichero de vídeo encriptado y el fichero de vídeo encriptado puede almacenarse en el aparato terminal de comunicación 20. Tan pronto entre el aparato terminal de comunicación 20 en la zona de actuación de una red potente, o sea por ejemplo en la zona de actuación de una red WLAN, pue-

de transmitirse el fichero de vídeo encriptado a un ulterior aparato de comunicación. El ulterior aparato de comunicación puede por ejemplo referirse al módulo central 10, a un servidor de ficheros, a un aparato terminal de comunicación de otro usuario o a cualquier otro ulterior aparato de comunicación.

REIVINDICACIONES

1. Procedimiento para la transmisión de datos, ejecutado por un módulo central (10), caracterizado porque comprende:

recepción de datos de autentificación (A) de un aparato terminal de comunicación (20),

almacenamiento de los datos de autentificación (A), estando dichos datos de autentificación (A) asociados a una identificación (iD),

generación de una llave electrónica (S), siendo dicha llave electrónica (S) almacenada de forma asociada a los datos de autentificación (A) y a la identificación (iD),

autentificación de la autorización a la llave electrónica (S) para el aparato terminal de comunicación (20) mediante los datos de autentificación (A) recibidos,

comprobación de una disponibilidad del aparato terminal de comunicación (20) mediante un módulo de disponibilidad del módulo central (10),

generación de datos encriptados (vD), mediante un módulo de encriptación, de datos (D) y de al menos una parte de la llave electrónica (S), siendo asociada a los datos (D) o los datos encriptados (vD) o a ambos la identificación (iD), y siendo almacenados los datos de autentificación (A) de forma asociada a la identificación (D),

transmisión de los datos encriptados (VD) y de al menos una parte de la llave electrónica (S) al aparato

terminal de comunicación (20), estando dicho aparato de comunicación (20) disponible y autorizado.

2. Procedimiento según la reivindicación 1, caracterizado porque en el módulo central (10) o en el aparato terminal de comunicación (20), respectivamente, se almacena un perfil de usuario, siendo seleccionados y encriptados datos según el perfil de usuario así como transmitidos al aparato terminal de comunicación (20) o a un ulterior aparato de comunicación, respectivamente.

3. Procedimiento según una de las reivindicaciones 1 a 2, caracterizado porque mediante un módulo de activación del módulo central (10) es activado un interfase de red del aparato terminal de comunicación (20) y porque los datos encriptados (vD) son transmitidos a través del interfase de red activado al aparato terminal de comunicación (20).

4. Procedimiento según una de las reivindicaciones 1 a 3, caracterizado porque los datos encriptados (vD) son transmitidos a un aparato de red de una infraestructura de red, siendo los datos encriptados (vD) almacenados en el aparato de red y transmitidos de forma asíncrona por el aparato de red al aparato terminal de comunicación (20).

5. Procedimiento según una de las reivindicaciones 1 a 4, caracterizado porque durante la transmisión de la al menos una parte de la llave electrónica (S) es cargado un importe dinerario en una cuenta de usuario.

6. Procedimiento según una de las reivindicaciones 1 a 5, caracterizado porque los datos encriptados (vD) comprenden un código de programa, cuyo código de programa debe ser eje-

cutado para la descodificación de los datos encriptados (vD), siendo comprobados criterios de validez durante la ejecución del código de programa.

7. Sistema para la transmisión de datos, caracterizado porque comprende un módulo central con medios para la realización de un procedimiento según la reivindicación 1.

8. Sistema según la reivindicación 7, caracterizado porque en el módulo central (10) o en el aparato terminal de comunicación (20), respectivamente, es almacenable un perfil de usuario, siendo datos seleccionables y encriptables según el perfil de usuario así como susceptibles de ser transmitidos a un aparato terminal de comunicación (20) o a un ulterior aparato de comunicación, respectivamente.

9. Sistema según una de las reivindicaciones 7 a 8, caracterizado porque mediante un módulo de activación del módulo central (10) es activable un interfase de red del aparato terminal de comunicación (20) y porque los datos encriptados (vD) son susceptibles de ser transmitidos a través del interfase de red activado al aparato terminal de comunicación (20).

10. Sistema según una de las reivindicaciones 7 a 9, caracterizado porque los datos encriptados (vD) son susceptibles de ser transmitidos a un aparato de red de una infraestructura de red, siendo los datos encriptados (vD) almacenables en el aparato de red y susceptibles de ser transmitidos de forma asíncrona por el aparato de red al aparato terminal de comunicación (20).

11. Sistema según una de las reivindicaciones 7 a 10,

caracterizado porque durante la transmisión de la al menos una parte de la llave electrónica (S) es cargable un importe dinerario en una cuenta de usuario.

12. Sistema según una de las reivindicaciones 7 a 11, caracterizado porque los datos encriptados (vD) comprenden un código de programa, cuyo código de programa es ejecutable obligadamente para la descodificación de los datos encriptados (vD), siendo comprobables criterios de validez durante la ejecución del código de programa.

Siguen tres láminas de dibujos.

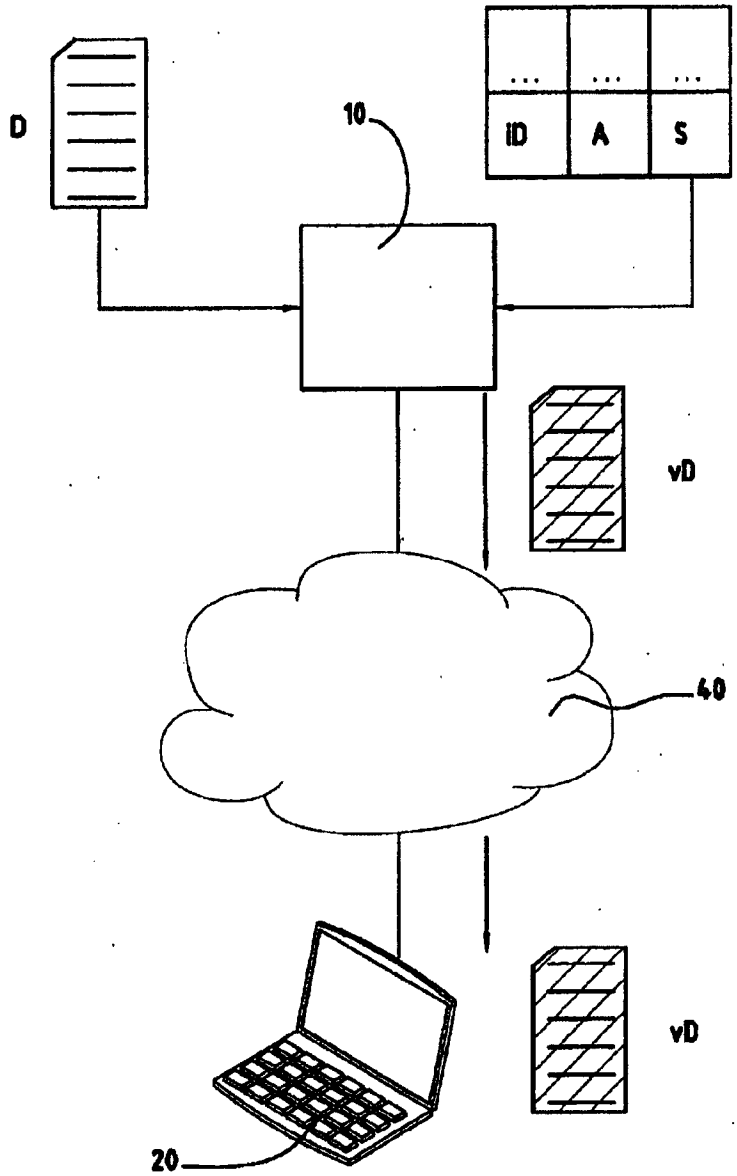

Fig. 1

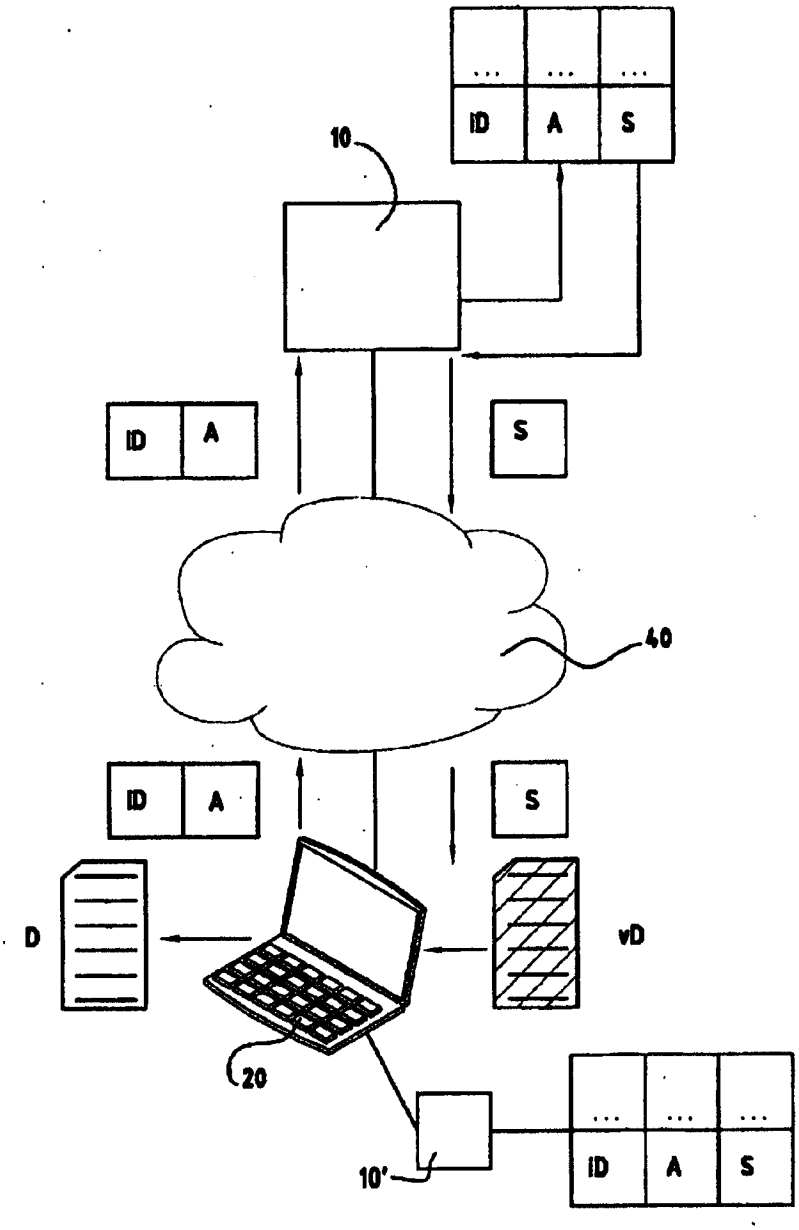

Fig. 2

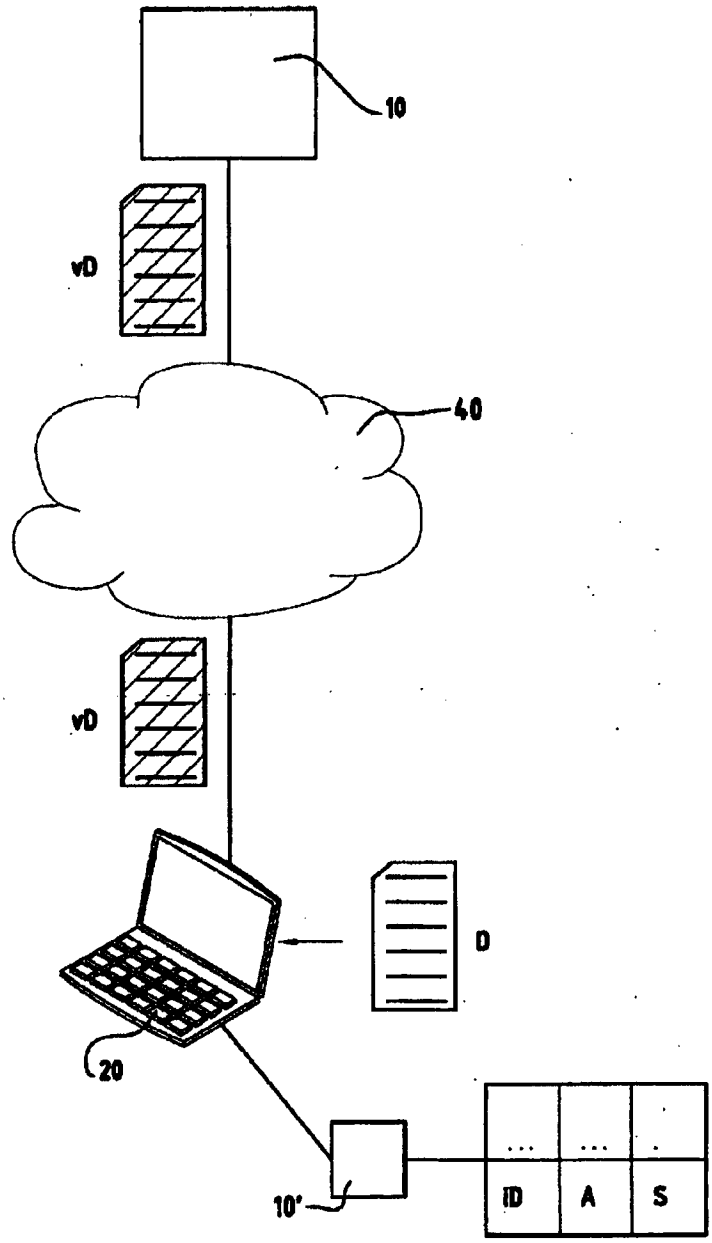

Fig. 3