(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 360 197**

(51) Int. Cl.:
H04L 12/24 (2006.01)
H04L 12/46 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **02751506 .3**
(96) Fecha de presentación : **22.07.2002**
(97) Número de publicación de la solicitud: **1413088**
(97) Fecha de publicación de la solicitud: **28.04.2004**

(54) Título: **Método para crear una red virtual privada utilizando una red pública.**

(30) Prioridad: **30.07.2001 CH 1424/01**

(45) Fecha de publicación de la mención BOPI:
01.06.2011

(45) Fecha de la publicación del folleto de la patente:
01.06.2011

(73) Titular/es: **NAGRAVISION S.A.**
22, route de Genève
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es: **Collet, Daniel**

(74) Agente: **Tomás Gil, Tesifonte Enrique**

DESCRIPCIÓN

Método para crear una red virtual privada utilizando una red pública.

La presente solicitud se refiere al campo de las redes informáticas, en particular, a la creación de una red privada al interior de una red pública.

Estas redes son conocidas según la denominación anglófona "Virtual Private Network" (red virtual privada) (VPN).

Se prevé que se establecerá un enlace protegido entre dos puntos a través de una red pública utilizando un protocolo de intercambio de claves para la creación de un enlace protegido. Dicho protocolo se describe en la norma SSL que está basada en el intercambio de datos gracias a un par de claves, que son la clave pública y la clave privada para la definición de una clave de sesión simétrica de codificación. Los datos están codificados por esta clave de sesión, siendo esta última utilizada únicamente para esta transacción.

Esta funcionalidad sólo puede desarrollarse entre dos interlocutores y no puede, por lo tanto, permitir la formación de una red de varios usuarios. En efecto, hay tantas unidades de diálogo como ordenadores a conectar.

La necesidad de crear este tipo de redes está presente cuando se desea conectar varios puntos distantes pero conectados a una misma red pública como, por ejemplo, Internet.

Esta necesidad es de igual importancia que la de una protección eficaz de los datos intercambiados porque en cuanto se lleva a cabo la conexión a Internet, no se garantiza ninguna confidencialidad.

De este modo, queda un problema por resolver que consiste en conectar varios ordenadores o unidades multimedia a través de una red pública garantizando al mismo tiempo el carácter confidencial de estos datos.

Este objetivo se alcanza mediante un método de creación y de explotación de una red privada virtual (VPN) que consta de una pluralidad de unidades conectadas a una red pública; cada unidad consta de los medios de seguridad que dispone de un número único UA1. Este método se caracteriza por las etapas siguientes:

- generar por los medios de seguridad de una unidad U1, un derecho D1 asociado al número único UA1,
- transferir este derecho D1 a los medios de seguridad de, al menos, una unidad U2,
- codificar los datos mandados por la unidad U1 y la descripción del derecho D1 por una primera clave K1,
- recibir los datos codificados por la segunda unidad U2, presentar estos datos a los medios de seguridad de la unidad U2, verificar si los derechos D1 están presentes y en caso afirmativo, descodificar los datos.

Cuando la unidad U2 desea comunicarse con la unidad U1, ejecuta la misma operación utilizando el derecho D1 como identificador y la unidad U1 podrá recibir los datos puesto que contiene este derecho.

Cuando la unidad U1 envía su derecho D1 a una tercera unidad U3, el mismo principio se aplica entre la unidad U1 y U3 pero también entre la unidad U2 y la unidad U3. Estas van a utilizar el derecho D1 iniciado por la unidad U1 para autorizar la descodificación de los datos.

Se constata de este modo que se ha creado una red espontánea cuyo gestor es la unidad U1 que es la que ha creado el primer derecho.

Se pueden dividir las unidades en dos categorías, las unidades generadoras como la unidad U1 y las unidades participantes como la U2 y la U3.

Se debe señalar que si la unidad U2 desea comunicarse con la unidad U1 sin que la unidad U3 pueda descodificar los datos, la unidad U2 convierte igualmente una unidad generadora y envía un derecho D2 a la unidad U1. Una segunda red virtual ha sido creada entre las unidades U1 y U2.

Prácticamente, estos medios de seguridad pueden presentarse bajo varias formas. Para asegurar una alta seguridad al mecanismo de codificación/descodificación, se utilizan los microprocesadores especializados que contienen el motor de codificación y de los datos tales como las claves de seguridad.

Estos microprocesadores están proporcionados bajo la forma de una tarjeta chip con formato Tarjeta SIM Plug-in o ISO 7816-2.

Según una primera variante de la invención, la tarjeta de red de las unidades contiene dicha tarjeta electrónica, por ejemplo de una manera equivalente a un teléfono GSM. Los datos son de este modo tratados directamente sobre la tarjeta de red y el funcionamiento se hace de manera transparente.

El usuario de la unidad U2, en el momento de la emisión de los datos, sólo tendrá que seleccionar la red por la cual se debe hacer la codificación. En efecto, puede que la unidad U2 sea miembro de varias redes (por ejemplo U1 y U3) y por lo tanto se tiene que efectuar una selección.

El envío del derecho D1 a otra unidad es una operación que requiere un gran cuidado. En efecto, hay que estar seguro de que este derecho sólo se carga en las unidades deseadas por U1. Por eso existen varias soluciones:

- la unidad U1 accede a la clave pública de la unidad U2 para codificar el derecho D1 y enviarlo a la unidad U2. Entonces, este derecho sólo puede ser descodificado por U2 gracias a su clave privada. Las otras unidades, que no poseen la clave privada de la unidad U2, no podrán descodificar el derecho D1.
- el protocolo de carga en los medios de seguridad exige la introducción de una contraseña. La unidad U1, en el momento de la generación del derecho D1, solicita al usuario una contraseña que está asociada con el derecho en forma codificada. Este derecho D1 es enviado a la unidad U2, y cuando el usuario de U2 solicita cargar este derecho en los medios de seguridad, estos últimos piden la introducción de la contraseña. Gracias a la clave secreta contenida en todos los módulos de seguridad, la contraseña está controlada por los contenido en el derecho D1 y el derecho sólo se carga si las contraseñas son idénticas. La contraseña es transmitida entre U1 y U2 por otros medios, por ejemplo, por teléfono. Una variante de esta solución consiste en enviar el derecho D1 mezclado con un gran número de datos de relleno. La contrase-

ña es entonces utilizada como clave de direccionamiento para extraer el derecho D1 en el interior de estos datos superfluos.

- un medio sencillo y eficaz es cargar el derecho D1 en un soporte amovible como un disquete y enviarlo a U2.
- el aparato huésped de los medios de seguridad dispone de un segundo emplazamiento en el cual es posible colocar un segundo medio de seguridad. La transferencia se efectúa de un medio hacia otro en un entorno restringido.

Con el fin de impedir que el derecho D1 pueda ser cargado en otras unidades a parte de la U2, es posible generar el derecho D1 y asociarle al número único de U2 (es decir UA2). La información D1, UA2 está mandada en U2 y si otros medios de seguridad (Un) intentan cargar este derecho (con la contraseña por ejemplo), una verificación se realiza con el fin de controlar si el número único UAn corresponde con el asociado al derecho D1.

Las claves utilizadas durante las diferentes transacciones desempeñan un papel importante. Para la clave de codificación de estos datos, pueden utilizarse varias variantes.

Según una primera variante, los medios de seguridad comprenden una clave secreta común en todos los medios de seguridad. Esta clave puede ser de tipo asimétrico (RSA) o simétrico (DES, CAST, IDEA).

Según una segunda variante, los medios de seguridad de la unidad U1 generan una clave de codificación/descodificación K1, lo codifican con la clave de servicio K0 y lo mandan con el derecho D1 según las modalidades detalladas más arriba. De este modo, habrá tantas claves diferentes como redes virtuales. Por lo tanto, una unidad que participa en tres redes va a almacenar tres claves diferentes de codificación.

En una forma más elaborada de la invención, es posible que la unidad U1 desee transmitir las informaciones con U3 sin que U2, igualmente miembro de su red, pueda leer estas informaciones. Por esta razón, cuando U1 genera el derecho D1, se agrega un índice de red. Este índice puede mantenerse sobre algunos bits si se desea limitar el número de redes creado por U1 a 256 por ejemplo, en cuanto a la unidad U2, si participa a varias redes iniciadas por U1, no duplicará el derecho D1 sino sencillamente el índice de la red.

Después de la fase de transmisión de este derecho a la unidad U2, los medios de seguridad van a proceder a la verificación del derecho y del índice. Se recuerda aquí que estos datos son almacenados en un criptoprocesador y no pueden ser modificados por el usuario.

De esta manera, será mucho mas fácil que la unidad U1 gestione las diferentes redes creadas.

Esta invención se extiende igualmente a un sistema de gestión centralizado de derechos. Todas las unidades son conectadas (o pueden serlo en un momento dado) a un centro de gestión. Cuando una unidad requiere la creación de una red R1, ésta envía esta solicitud al centro de gestión.

Este verifica si la unidad está habilitada para realizar esta operación y en caso afirmativo, reenvía a la unidad 1 el derecho D1 y una clave K1 de codificación propia a la red R1.

Cuando la unidad U2 desea participar en esta red, la unidad U1 transmite el derecho D1 o una parte de este derecho a la unidad U2 según las modalidades ya mencionadas arriba. Con este derecho, la unidad U2 puede solicitar a este centro de gestión con el objeto de recibir la clave K1 y el derecho D1 en su conjunto.

Si se hace referencia aquí a una parte del derecho D1 que está trasladada de la unidad U1 a la unidad U2, esto viene del hecho de que el derecho D1 está transmitido en su totalidad a la unidad U2 por el centro de gestión. Se puede imaginar que la unidad U1, cuando se crea la red R1, le atribuye una contraseña. Esta contraseña, representativa del derecho D1 es transmitida a la unidad U2 que él mismo le presenta al centro de gestión.

El centro verifica la contraseña y si es correcta, el derecho D1 es transmitido a la unidad U2.

El interés de un centro de gestión es la gestión dinámica de tal red. En efecto, el problema de la radiación de un miembro de una red puede ocurrir en cualquier momento. Además, un nivel de seguridad elevado implica el cambio frecuente de las claves de codificación.

Estas funcionalidades están disponibles por el centro de gestión que puede coordinar un cambio de clave para una red dada. La nueva clave se transmite a todas las unidades de esta red gracias al enlace protegido que conecta las unidades al centro de gestión. Este tipo de datos es transmitido codificado con destinatario el número único de cada unidad. De esta manera, es posible retirar un miembro del grupo dejando de transmitirle las actualizaciones de las claves. El centro puede radiar un miembro mandando una orden de desactivación del derecho.

La invención se entenderá mejor gracias a la descripción detallada a continuación, la cual se refiere a los dibujos anexos que son dados en calidad de ejemplo de ningún modo limitativo, es decir:

- la figura 1 describe una red sin centro de gestión a un sólo nivel
- la figura 2 describe una red sin centro de gestión a varios niveles,
- la figura 3 describe una red con centro de gestión.

La figura 1 ilustra 5 unidades identificadas UN1 a UN5. Cada unidad contiene medios de seguridad en los cuales se halla un cripto-procesador encargado de la generación de los derechos.

Según nuestro ejemplo, la unidad UN1 genera el derecho D1 que envía a las unidades UN2 y UN4.

Paralelamente, la unidad UN5 genera un derecho D5 que envía a las unidades UN2 y UN3.

Tenemos una primera red formada por las unidades UN1, UN2 y UN4 así como una segunda red formada por las unidades UN2, UN3 y UN5. La unidad UN2 deberá seleccionar la red sobre la que desea trabajar ya que dispone de los dos derechos.

Cuando los datos son intercambiados entre estas diferentes unidades, existen dos maneras de operar. Según un primer modo de realización, la clave secreta contenida en los medios de seguridad (o aquella generada con el derecho) está utilizada para codificar todos los contenidos transferidos entre las diferentes unidades. Otra manera consiste en utilizar una clave de sesión.

Esta clave de sesión aleatoria KS está generada por la unidad emisora, y sirve para codificar los datos. Por razones operacionales de rapidez, esta clave es de tipo simétrico. La unidad emisora tiene un bloque de datos de control que consta de la clave de sesión KS

y de la definición del derecho necesaria para la descodificación de los datos. Este bloque está codificado por una clave de servicio común a las unidades, o por la clave generada con el derecho D.

En el momento de la recepción, el bloque de control está tratado por los medios de seguridad previamente al tratamiento de los datos. Por lo tanto, estos medios van a descodificar el bloque de control y verificar si el derecho pedido está presente en esta unidad. En caso afirmativo, la clave de sesión KS es aplicada a los datos que permiten descodificarla.

La figura 2 ilustra una variante en la cual la unidad UN1 ha generado dos derechos para crear dos redes, D1a y D1b. Una primera red está creada entre las unidades UN1, UN2 y UN3 mientras una segunda red está creada ente las unidades UN1, UN4 y UN5.

Esta variante permite una gran flexibilidad en la difusión de las informaciones confidenciales eligiendo cual podrá descodificar las informaciones. En efecto, puesto que la red de transmisión es pública, se considera que las informaciones son accesibles a todas las unidades que disponen del derecho aun cuando el enlace se hace de una unidad hacia el otra.

La figura 3 representa la variante con un centro de gestión CG. La unidad UN1 requiere del centro CG el derecho D1 así como de la clave de codificación k1. El centro registra la creación de la red R1 en su base de datos. La unidad UN2 para participar a esta red debe igualmente recibir este derecho D1. Por eso, el método utilizado puede ser aquel descrito ulteriormente o puede recibir el soporte del centro de gestión. En efecto, según un protocolo particular, la unidad UN1 puede comunicar la dirección de las unidades con las cuales desea crear la red R1. El centro de gestión CG, gracias a los medios de telecomunicación asegurados que incluye, va a transferir el derecho D1 a todas las unidades referidas así como la clave k1 de codificación/descodificación. De una manera similar, si la unidad UN3 desea crear una red R3, pide al centro de gestión que le atribuya la red R3 asociada al derecho D3.

El conocimiento de todas las unidades que participan en una red dada es importante para el cambio regular de las claves de codificación. El centro CG puede cambiar las claves en las unidades a intervalos regulares (o pseudo-aleatorios) para evitar utilizar la misma clave demasiado tiempo, lo cual la haría vulnerable.

El cambio de clave también es muy práctico para eliminar un miembro de la red. La unidad generadora UN1 informa al centro de gestión CG que la unidad UNn ya no forma parte de la red D1 y el centro deja de comunicar las nuevas claves. Alternativamente o como complemento, puede enviar una orden de desactivación a esta unidad.

Esta clave K1 puede ser de tipo simétrico o asimétrico. En el segundo caso, cada unidad dispone de las dos claves privadas y públicas y al codificarse o descodificarse, cualquiera de las claves será utilizada.

En el momento de la transmisión de datos, éstas son generalmente codificadas por una clave de sesión generada aleatoriamente. Esta clave es luego codificada por la clave K1 antes de ser transmitida a las otras unidades.

Según un modo de realización de la invención, las unidades UN son descodificadores de televisión de pago y los medios de seguridad están constituidos por la tarjeta chip. Estos descodificadores sirven igualmente para recibir y enviar los datos para los mensajes electrónicos por ejemplo. Es igualmente posible conectar tal descodificador a un ordenador para beneficiarse de la interfaz con una red de alta velocidad por una parte y de la seguridad de las transacciones por otra parte.

Según un modo de realización particular, el derecho D incluye un campo de validez. De este modo, cada unidad que recibe este derecho dispone de un periodo de validez. A cada intercambio de datos, (ver bloque de control más arriba), la fecha corriente se agrega. Se recuerda que este bloque de control está codificado.

Los medios de seguridad verifican la conformidad de la validez del derecho D con la fecha contenida en el bloque de control. Si esta fecha está fuera de la validez, la descodificación de los datos no se efectúa. Según el modo elegido, ya sea con una unidad fija o con un centro de gestión, se prevé renovar la validez antes del plazo en el caso claro de que el gestor del derecho le necesite para la unidad considerada. Esta renovación se efectúa mediante el envío de un mensaje de control a las unidades referidas con la descripción del derecho y la nueva validez. Una vez que la validez esté superada, el derecho ya no puede extenderse y un nuevo procedimiento de transmisión del derecho, tal y como descrita más arriba, es necesario.

REIVINDICACIONES

1. Método para crear y explotar una red virtual privada (VPN) que comprende una pluralidad de unidades conectadas a una red pública, cada unidad comprende medios de seguridad que disponen al menos de un número único UA, método **caracterizado** por las siguientes etapas que consisten en:

- generar por los medios de seguridad de una unidad Un, un derecho Dn asociado a un número único UAn,
- transferir de manera segura y almacenar este derecho Dn en los medios de al menos una unidad Um,
- codificar por la unidad Un los datos a enviar y la descripción del derecho Dn por una clave de codificación de datos KS que es o bien una primera clave Kn común en los medios de seguridad Un y Um, o una clave de sesión generada aleatoriamente por la unidad Un y codificada por la primera clave común Kn, esta clave de sesión codificada siendo adjuntada a los datos codificados y al derecho Dn,
- recibir datos codificados por la segunda unidad Um, presentarlos a los medios de seguridad de la unidad Um, descodificar la descripción del derecho Dn y verificar si la descripción del derecho Dn corresponde al derecho Dn almacenado y en caso afirmativo, codificar los datos por la clave de codificación de datos KS.

2. Método según la reivindicación 1, **caracterizado** por el hecho de que el derecho Dn está asociado con un identificador de la segunda unidad Um, y de que los medios de seguridad de la segunda unidad verifican que el derecho Dn está destinado a ellos.

3. Método según las reivindicaciones 1 o 2, **caracterizado** por el hecho de que la unidad Un asocia un índice de red RA con el derecho Dn, y que la pertenencia de otra unidad se efectúa según los criterios del derecho Dn y del índice de red RA.

4. Método según la reivindicación 1, **caracterizado** por el hecho de que la primera clave Kn se genera con el derecho Dn y se transmite a las unidades participantes por medio de una clave de servicio secreta KO común de los medios de seguridad.

5. Método según las reivindicaciones 1 a 4, **caracterizado** por el hecho de que el derecho Dn incluye un campo de validez, y comprende las siguientes etapas que consisten en

- adjuntar a la descripción del derecho Dn, una indicación de la fecha actual de forma codificada por la unidad Un,
- recibir esta indicación por la unidad Um y verificar por los medios de seguridad de la unidad Um que esta fecha se incluye en la duración de la validez del derecho Dn.

6. Métodos para crear y explotar una red privada virtual (VPN) que comprende una pluralidad de unidades conectadas a un centro de gestión (CG) a través de una red pública, cada unidad comprendiendo medios de seguridad que disponen al menos de un número único UA, este método siendo **caracterizado** por las siguientes etapas que consisten en:

- solicitar por la unidad Un al centro de gestión (CG), la creación de una red Rn,
- enviar de manera segura por el centro de gestión (CG) a la unidad Un, un derecho Dn y una clave Kn que representa una red Rn,
- solicitar la inscripción en el centro de gestión de la unidad Um como miembro de la red Rn,
- transmitir de manera segura y almacenar por medio de la unidad Um, el derecho Dn y la clave Kn,
- codificar por la unidad Un los datos a enviar y la descripción del derecho Dn por una clave de codificación de los datos KS, esta clave de codificación KS siendo o bien una clave Kn común a las unidades Un y Um, o una clave de sesión generada aleatoriamente por la unidad Un y codificada por la clave común Kn, esta clave de sesión codificada siendo adjuntada a los datos codificados y al derecho Dn,
- recibir los datos codificados por la segunda unidad Um, presentar estos datos a los medios de seguridad de la unidad Um, descodificar la descripción del derecho Dn y verificar si la descripción del derecho Dn corresponde al derecho Dn almacenado y en caso afirmativo, descodificar los datos por la clave de codificación de los datos KS.

7. Método según la reivindicación 6, **caracterizada** por el hecho de que la solicitud de inscripción de la unidad Um comprende las siguientes etapas de:

- transmisión por la unidad Un de una parte que representa el derecho Dn,
- presentación por la unidad Um de esta parte de derecho Dn al centro de gestión,
- verificación por el centro de gestión (CG) que esta parte corresponde al derecho Dn y transmisión del derecho Dn y de la clave Kn a la unidad Um en caso afirmativo.

8. Método según la reivindicación 6, **caracterizado** por el hecho de que la solicitud de inscripción de la unidad Um comprende las siguientes etapas de:

- transmisión por la unidad Um del identificador de la unidad Um al centro de gestión (CG),
- transmisión por el centro de gestión del derecho Dn y de la clave Kn a la unidad Um.

9. Método según la reivindicación 6, **caracterizado** por el hecho de que el centro de gestión (CG) envía a miembros de una misma red Rn una nueva clave Kn' con un intervalo pseudo-aleatorio.

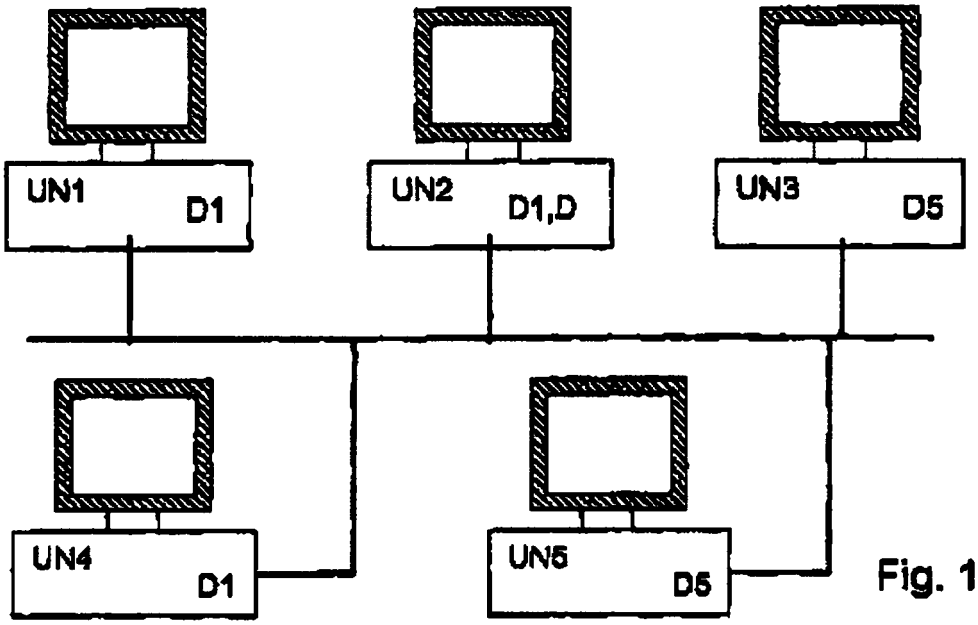
UN1
D1
UN2
D1,D
UN3
D5
UN4
D1
UN5
D5

Fig. 1

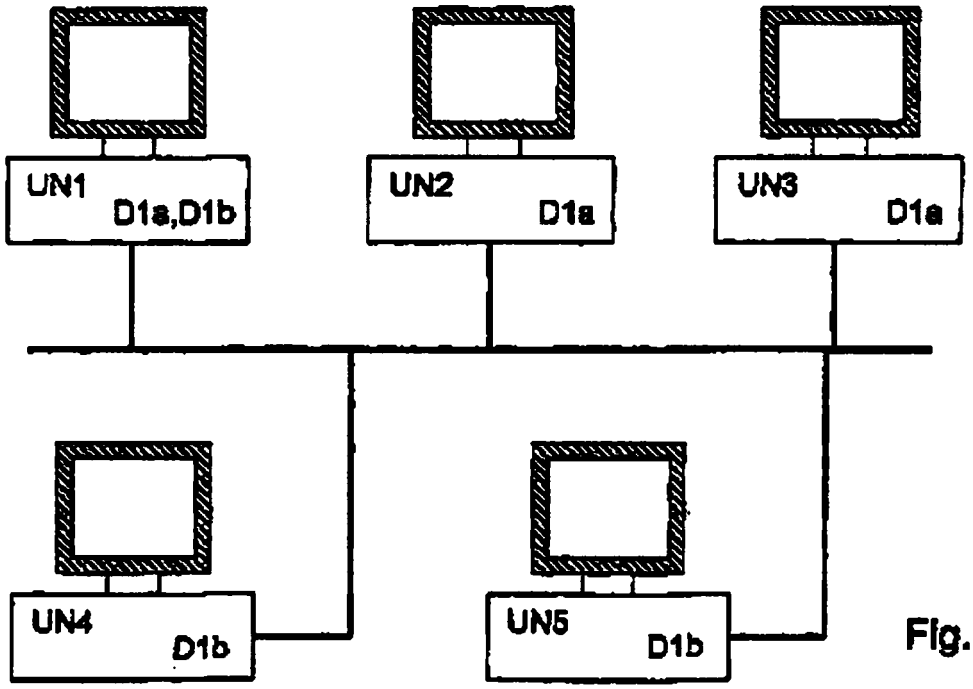
UN1
D1a,D1b
UN2
D1a
UN3
D1a
UN4
D1b
UN5
D1b

Fig. 2

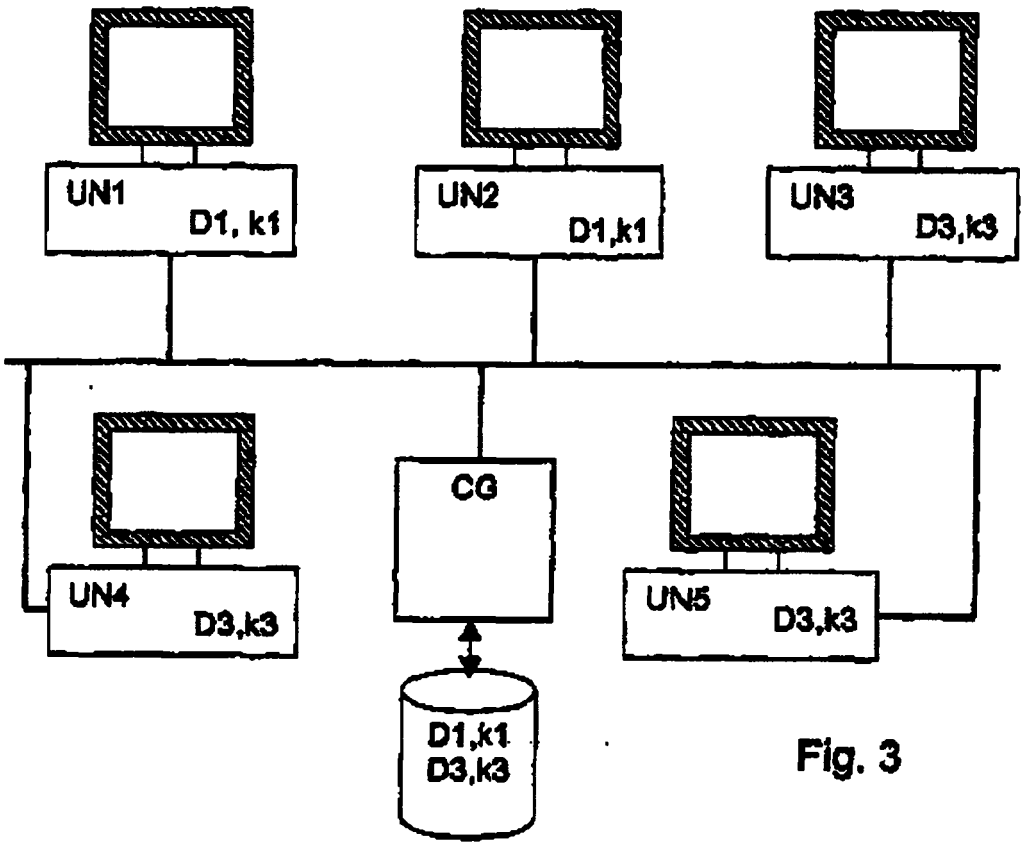

Fig. 3