(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 379 074**

(51) Int. Cl.:
H04L 29/06 (2006.01)
H04L 12/28 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05102294 .5**
(96) Fecha de presentación : **22.03.2005**
(97) Número de publicación de la solicitud: **1705855**
(97) Fecha de publicación de la solicitud: **27.09.2006**

(54) Título: **Método y sistema para el establecimiento de un canal de comunicaciones de tipo "peer-to-peer".**

(45) Fecha de publicación de la mención BOPI:
20.04.2012

(45) Fecha de la publicación del folleto de la patente:
20.04.2012

(73) Titular/es: **Swisscom AG.**
Alte Tiefenaustrasse 6 Worblaufen/Ittigen
3050 Bern, CH

(72) Inventor/es: **De Froment, Eric**

(74) Agente/Representante:
Carvajal y Urquijo, Isabel

DESCRIPCIÓN

Método y sistema para el establecimiento de un canal de comunicaciones de tipo “peer-to-peer”.

Ámbito técnico

La presente invención se refiere a un método y un sistema para el establecimiento dinámico de un canal de comunicaciones entre un primer terminal y un segundo terminal, en que el primer terminal está conectado a través de un primer canal de comunicaciones securizado a una red securizada, y en que el segundo terminal está conectado a través de un segundo canal de comunicaciones securizado a la red securizada.

Estado de la técnica

Dispositivos móviles -especialmente dispositivos móviles con más de un interfase de red- son empleados cada vez más extensamente por usuarios móviles o nomádicos para por ejemplo acceder, leer, escribir, manipular, o almacenar diferentes tipos de datos. Dispositivos móviles comprenden, por ejemplo, teléfonos celulares, asistentes digitales personales, u ordenadores personales móviles, que también son conocidos como notebooks o portátiles. Interfases de red comprenden, por ejemplo, interfases de red alámbricos para acceder por ejemplo a Local Area Network (LAN), módems para acceder a redes remotas a través de por ejemplo una red telefónica fija o Public Switched Telephone Network (PSTN), o interfases de red inalámbricos para acceder por ejemplo a una red de área local inalámbrica o Wireless Local Area Network (WLAN). Usuarios de dispositivos móviles pueden leer y escribir mensajes de e-mail o documentos de texto, o pueden acceder o manipular datos multimedia tales como imágenes, datos de audio, o datos de vídeo. Así por ejemplo, un comercial de una empresa que esté visitando un cliente también tiene necesidad de acceder a datos securizados, de confianza de su empresa. Con el fin de acceder a datos securizados, un dispositivo móvil puede conectarse a través de una conexión securizada a un “gateway” de seguridad de una red de empresa. Tales conexiones securizadas comprenden, por ejemplo, conexiones autenticadas y encriptadas que empleen el protocolo IPsec (IPsec: Internet Protocol secured) o el protocolo SSL (SSL: Secured Socket Layer). Así por ejemplo, un comercial con necesidad de acceder a datos securizados de su empresa puede conectar su dispositivo móvil a una red del cliente, por ejemplo mediante una red WLAN. La red WLAN puede proporcionar acceso a Internet. El “gateway” de seguridad de la red de empresa, por ejemplo, está configurado para recibir conexiones IPsec desde Internet. Tan pronto se ha conectado el comercial con su dispositivo móvil a través de un canal de comunicaciones securizado, tal como una conexión IPsec, con el “gateway” de seguridad de su empresa, el dispositivo móvil puede convertirse en parte de la red de la empresa, y puede beneficiarse de diversos derechos de acceso a datos de empresa almacenados en ordenadores o servidores de la empresa. En otras palabras, el dispositivo móvil del comercial constituye, al menos hasta cierto punto, parte de la red de la empresa del comercial. A través del “gateway” de seguridad de la empresa los dispositivos móviles son conectables a la red de la empresa desde diversas ubicaciones. Por consiguiente, un comercial que emplee su dispositivo móvil en una primera ubicación y un asesor técnico que emplee su dispositivo móvil en una segunda ubicación, por ejemplo, son capaces -a través de la red securizada- de acceder a datos en cada dispositivo móvil del otro. Sin embargo, es un inconveniente que todo el tráfico entre los dispositivos móviles deba pasar a través de la red de la empresa, incluso si, por ejemplo, los dispositivos móviles del comercial y del asesor técnico fueran conectables a través de una ulterior red, quizá más eficiente. Un ulterior inconveniente consiste en que la red securizada de la empresa puede resultar comprometida o interrumpida si, por ejemplo, el comercial y el asesor técnico deciden configurar sus dispositivos móviles para establecer un canal de comunicación “peer-to-peer” entre sus dispositivos móviles. Es también un inconveniente el que la transferencia de datos -a través de la red securizada- entre dispositivos móviles requiera múltiples encapsulamientos de datos que disminuyen el rendimiento de la transferencia de datos y el que el “gateway” de seguridad de la red securizada pueda resultar un cuello de botella debido a la concentración de carga de tráfico.

En el documento XP 2314796 se describe el establecimiento de un canal de comunicación directa entre un primer y un segundo terminal para enviar marcos directamente entre los terminales en lugar de a través del punto de acceso.

Descripción de la invención

Constituye la finalidad de la presente invención proponer un nuevo método y sistema para el establecimiento dinámico de un canal de comunicaciones entre un primer terminal y un segundo terminal, en que el primer terminal está conectado a través de un primer canal de comunicaciones securizado con una red securizada, y en que el segundo terminal esté conectado a través de un segundo canal de comunicaciones securizado con la red securizada, cuyos método y sistema no adolezcan de los inconvenientes del estado de la técnica.

Estas finalidades se consiguen, de acuerdo con la presente invención, mediante los elementos de las reivindicaciones independientes. Ulteriores formas de realización preferidas se desprenden, además, de las reivindicaciones dependientes y de la descripción.

Las finalidades arriba citadas se consiguen mediante la presente invención por el hecho de que el primer terminal genera una solicitud de conexión para el establecimiento de un canal de comunicaciones entre el primer y el segundo terminal, de que la solicitud de conexión es recibida y analizada por un módulo analizador, de que los parámetros de red del primer terminal y del segundo terminal son recibidos y analizados por el módulo analizador, y de que el módulo analizador, basado en el análisis de la solicitud de conexión y de los parámetros de red de los terminales, transmite una instrucción de conexión al primer y/o segundo terminal para el establecimiento de un canal de comunicaciones "peer-to peer" -a través de una red distinta de la red securizada- entre el primer terminal y el segundo terminal. La presente invención presenta la ventaja de que la transferencia de datos, especialmente entre dispositivos móviles, puede realizarse de manera más eficiente estableciendo dinámicamente un canal de comunicaciones "peer-to-peer" entre los respectivos terminales. La presente invención presenta la ulterior ventaja de que el tráfico de red a y desde una red de empresa puede ser reducido, dando especialmente lugar a menos problemas de cuello de botella para "gateways" de seguridad de la red de empresa.

De acuerdo con una variante de realización, el canal de comunicaciones "peer-to-peer" entre el primer terminal y el segundo terminal es establecido como un canal de comunicaciones securizado "peer-to-peer" por medio de módulos de autenticación y/o encripción. Así por ejemplo, datos criptográficos comprendiendo claves de autenticación y claves de encripción pueden ser proporcionados por el módulo analizador a módulos de autenticación y/o de encripción del primer y segundo terminal, de manera que el canal de comunicaciones "peer-to-peer" entre el primer y el segundo terminal pueda ser establecido de acuerdo con condiciones de seguridad definidas. Una tal variante de realización posee la ventaja de que puedan cumplirse condiciones de seguridad de la red securizada.

De acuerdo con otra variante de realización son proporcionadas claves de autenticación y/o encripción a los módulos de autenticación y/o encripción por una unidad central de la red securizada. Una tal variante de realización presenta la ventaja de que las claves de autenticación y/o encripción puedan ser proporcionadas de acuerdo con condiciones de seguridad definibles de la red securizada.

De acuerdo con otra variante de realización, la unidad central recibe parámetros sobre un estado del primer terminal y/o del segundo terminal a intervalos de tiempo determinables, y un canal de comunicaciones "peer-to-peer" establecido es interrumpido tan pronto el estado del primer y/o segundo terminal no cumplan condiciones determinables. Una tal variante de realización posee la ventaja de que la seguridad de la red securizada puede ser mejorada interrumpiendo canales de comunicaciones "peer-to-peer" entre terminales que no estén ya plenamente conectados a la red securizada, por ejemplo cuando el primer canal de comunicaciones securizado entre el primer terminal y la red securizada no sea ya operativo.

De acuerdo con una ulterior variante de realización, la solicitud de conexión generada por el primer terminal es interceptada por el módulo analizador. Cuando la solicitud de conexión es interceptada por el módulo analizador, la solicitud de conexión no es enviada a través de uno de los interfases de red del primer terminal, sino que la solicitud de conexión es retenida en el módulo analizador. Una tal variante de realización posee la ventaja de que la transferencia de datos entre el primer y el segundo terminal puede ser tratada de manera transparente, por ejemplo que el módulo analizador almacene la solicitud de conexión y que la solicitud de conexión sea enviada -eventualmente en formato modificado- a través del canal de comunicaciones "peer-to-peer" establecido dinámicamente entre el primer y el segundo terminal.

De acuerdo con otra variante de realización, el primer y el segundo canal de comunicaciones securizado entre el primer terminal y la red securizada y entre el segundo terminal y la red securizada son establecidos empleando puntos de acceso públicos para la conexión de los terminales a redes públicas, empleando canales de comunicaciones entre las redes públicas y la red securizada, y empleando módulos criptográficos para la autenticación de los terminales y para la encripción de los canales de comunicaciones entre los terminales y la red securizada. Así por ejemplo, la red pública es el Internet. Una tal variante de realización posee la ventaja de que usuarios de dispositivos móviles puedan beneficiarse de canales de comunicaciones "peer-to-peer" establecidos dinámicamente en una gran variedad de ubicaciones.

De acuerdo con otra variante de realización, el canal de comunicaciones "peer-to-peer" entre el primer terminal y el segundo terminal es establecido empleando al menos una red pública. Así por ejemplo, la red pública es el Internet. Una tal variante de realización posee la ventaja de que usuarios de dispositivos móviles puedan beneficiarse de una red ampliamente disponible y potente para el establecimiento de conexiones "peer-to-peer". Así por ejemplo, para una red securizada ubicada en Europa y para terminales móviles ubicados en América, las comunicaciones entre terminales móviles pueden resultar mucho más eficientes.

De acuerdo con otra variante de realización, el canal de comunicaciones "peer-to-peer" entre el primer terminal y el segundo terminal es establecido a través de una red *ad-hoc* entre el primer terminal y el segundo terminal. Así por ejemplo, la red *ad-hoc* está basada en una red Bluetooth. Una tal variante de realización posee la ventaja de que usuarios de dispositivos móviles que se hallen próximos entre sí puedan beneficiarse de recursos de red localmente disponibles. Así por ejemplo, terminales móviles ubicados en un tren y conectados a través de GPRS (General Packet Radio Service) con una red securizada pueden conectarse de manera más eficiente a través de una red *ad-hoc* Bluetooth.

Breve descripción de los dibujos

A continuación se describirá una forma de realización de la presente invención con referencia a un ejemplo. El ejemplo de esta forma de realización se ilustra en el dibujo adjunto, en el cual:

La Fig. 1 muestra un diagrama de bloques que representa esquemáticamente un sistema para el establecimiento dinámico de un canal de comunicaciones "peer-to-peer" entre un primer terminal (1) y un segundo terminal (2).

Modo(s) de realización de la invención

Con relación a la Fig. 1, el número de referencia 1 se refiere a un primer terminal, y el número de referencia 2 se refiere a un segundo terminal. El primer terminal 1 y el segundo terminal 2 son preferiblemente dispositivos móviles portátiles con al menos un interfase de red. El número de referencia 3 se refiere a interfases de red del primer terminal 1 y el número de referencia 4 se refiere a interfases de red del segundo terminal 2. Los interfases de red de los terminales 1, 2, tales como por ejemplo de notebooks o portátiles, pueden comprender un interfase de red 3, 4 para la conexión a una red alámbrica, por ejemplo de acuerdo con un IEEE802.3 Ethernet Standard, un interfase de red para la conexión a redes distantes a través de una red telefónica pública, por ejemplo mediante un módem, un interfase de red para la conexión a una red de área local inalámbrica, por ejemplo de acuerdo con un IEEE802.11 standard, un interfase de red para la conexión a una red móvil basada en GSM (Global System Mobile) o UMTS (Universal Mobile Telecommunications System), así como un interfase de red para la conexión directa con dispositivos ubicados en las cercanías, por ejemplo de acuerdo con un estándar Bluetooth o IrDA (Infrared Data Association).

Con relación a la Fig. 1, el número de referencia 9 se refiere a una red securizada. Una red puede ser considerada como una red securizada si las líneas principales, conexiones, conmutadores, cables, routers, etc. pertenecientes a la red son operados de acuerdo con condiciones definidas, por ejemplo de acuerdo con una política de seguridad y/o de acuerdo con directrices de seguridad de una empresa. La red securizada 9 comprende medios técnicos, por ejemplo controles de acceso a edificios con dispositivos de red, para proporcionar seguridad y está, o puede estar, conectada únicamente con dispositivos securizados. Un dispositivo puede ser considerado como securizado si, por ejemplo, el dispositivo está configurado de acuerdo con especificaciones definidas, por ejemplo empleando un sistema operativo de confianza, y/o instalando el dispositivo en el interior de edificios definidos, por ejemplo en el interior de edificios con únicamente acceso restringido, de una empresa. Acceso remoto securizado a la red securizada 9 puede conseguirse por medio de un "gateway" de seguridad, por ejemplo por medio de un concentrador IPsec.

Con relación a la Fig. 1, los números de referencia 5, 6 se refieren a redes apropiadas para un acceso remoto securizado de terminales 1, 2 a la red securizada 9, por ejemplo a la red de un Internet Service Provider, a una red WLAN, o a cualquier otra red. Tal como se ilustra en la Fig. 1, las redes 5, 6 son susceptibles de ser conectadas a una red securizada 9. La conexión entre una red 5, 6 y la red securizada 9 puede comprender enlaces directos, por ejemplo líneas de abonado ADSL (ADSL: Asynchronous Digital Subscriber Loop), líneas alquiladas, o cualquier otra conexión de red, o cualquier número de redes intermedias, por ejemplo redes de varios Internet Service Providers interconectados. Las redes 5, 6 pueden ser consideradas como parte del Internet público, mientras que la red securizada 9 puede ser considerada como una red securizada particular de una empresa susceptible de conectarse al Internet público. Así por ejemplo, una conexión originada por la red 5 y que penetre en la red securizada 9 puede ser obligada a terminar en el "gateway" de seguridad de la red securizada 9. Por medio del "gateway" de seguridad de la red securizada 9 cualquier conexión procedente de las redes 5, 6 es tratada de acuerdo con criterios definibles. Tales criterios pueden comprender autenticación del generador de la conexión y requisitos con respecto a algoritmos de encripción de datos.

Con relación a la Fig. 1, el primer terminal 1 está conectado por medio de uno de los interfases de red 3 a un punto de acceso de la red 5, por ejemplo mediante un módem. El segundo terminal 2 está conectado por medio de uno de los interfases de red 4 a un punto de acceso de la red 6, por ejemplo mediante un interfase de red inalámbrico. Por consiguiente, resulta establecida una conexión física para el transporte de paquetes de datos entre los terminales 1, 2 y la red securizada 9. De acuerdo con criterios definibles, los terminales 1, 2 establecen canales de comunicaciones securizados, por ejemplo conexiones IPsec, con el "gateway" de seguridad de la red securizada 9. Desde el "gateway" de seguridad tanto el primer terminal 1 como el segundo terminal 2 pueden recibir cada uno identificaciones de red definibles, por ejemplo números IP y nombres de servidor. Los terminales 1 y 2 pueden entonces participar plena o parcialmente como terminales de la red securizada 9 y pueden beneficiarse de todos los derechos y servicios de política proporcionados dentro de la red securizada 9. Así por ejemplo, primeros derechos de política pueden conceder al segundo terminal 2 el derecho a compartir datos definibles, y segundos derechos de política pueden conceder al primer terminal 1 el derecho a acceder a datos compartidos del segundo terminal 2. Por consiguiente, el primer terminal 1 puede solicitar una transferencia de datos del segundo terminal 2, cuyos datos resultarán entonces transferidos de forma segura por medio de la red securizada 9, por ejemplo a través de la red 6, a través del "gateway" de seguridad de la red securizada 9, y a través de la red 5. Una tal transferencia de datos comprende típicamente una encripción y encapsulación - de acuerdo con por ejemplo la conexión IPsec entre el segundo terminal 2 y el "gateway" de seguridad - de datos en el segundo terminal 2, una desencapsulación y desencripción de datos en el "gateway" de seguridad, una encripción y encapsulación - de acuerdo con por ejemplo la conexión IPsec entre el primer terminal 1 y el "gateway" de seguridad - de datos en el "gateway" de seguridad, y una desencapsulación y desencripción de datos en el primer terminal 1.

Con relación a la Fig. 1, el número de referencia A se refiere a un módulo analizador de acuerdo con la invención. En la Fig. 1 el módulo analizador A es susceptible de ser conectado a la red securizada 9. El módulo analizador A es capaz de analizar datos enviados y/o recibidos por los terminales 1 ó 2. Como tal, el módulo analizador A puede ser colocado en cualquier ubicación apropiada en el camino de datos entre los terminales 1 y 2. Así por ejemplo, el módulo analizador A puede ser conectable al "gateway" de seguridad de la red securizada 9, o el módulo analizador A puede ser conectable a los interfases de red 3, 4 de los terminales 1, 2. Preferiblemente, el módulo analizador A está diseñado como un módulo de software que controla una unidad procesadora, por ejemplo un microprocesador del "gateway" de seguridad de la red securizada 9 o un microprocesador de los terminales 1, 2.

El módulo analizador A comprende un módulo para analizar datos enviados y recibidos por los terminales 1, 2 y también un módulo para recibir y analizar parámetros de los terminales 1, 2. Al analizar paquetes de datos enviados y recibidos por los terminales 1, 2, el módulo analizador A busca una solicitud de conexión, por ejemplo busca encabezamientos de paquetes de datos en cuanto a diseños definibles tales como un puerto de destino configurado para compartir datos del segundo terminal 2. Así por ejemplo, tan pronto se detecta una solicitud de conexión, el módulo analizador A envía a los terminales 1, 2 una solicitud para recibir parámetros de dichos terminales. Correspondientes parámetros de los terminales 1, 2 son entonces recibidos por el módulo analizador A. Los parámetros de los terminales 1, 2 pueden también ser recibidos en cualquier otro instante, por ejemplo cada minuto. La solicitud para la recepción de parámetros de los terminales 1, 2 puede también comprender instrucciones tales que los terminales 1, 2 envíen apropiados parámetros tan pronto sean detectables cambios en dichos parámetros. Los parámetros de los terminales 1, 2 pueden incluir parámetros de los interfases de red 3, 4, por ejemplo parámetros que describan un tipo de interfase de red, por ejemplo alámbrico o inalámbrico, una velocidad de transmisión del interfase de red, una carga del interfase de red, redes conectables por el interfase de red, o cualquier otro parámetro que describa características del interfase de red 3, 4 ó de los terminales 1, 2. Al analizar los parámetros de los terminales 1, 2, el módulo analizador A puede comparar parámetros del interfase de red 3 con parámetros del interfase de red 4, y puede buscar al menos una red distinta de la red securizada 9 que sea adecuada para establecer un canal de comunicaciones "peer-to-peer" entre el primer y el segundo terminal 1, 2. Así por ejemplo, el módulo analizador puede detectar que uno de los interfases de red 3 es conectable con una red WLAN y que uno de los interfases de red 4 es conectable con la misma red WLAN. El trabajo de búsqueda de un canal de comunicaciones "peer-to-peer" adecuado puede también realizarse independientemente por los terminales 1, 2, eventualmente con la ayuda del módulo analizador A. El módulo analizador A puede también detectar que ambos terminales 1, 2 tengan una conexión a Internet. En cualquier caso, el módulo analizador A envía datos de configuración al primer y/o segundo terminal para configurar y establecer un canal de comunicaciones "peer-to-peer" a través de una red que sea distinta de la red securizada 9. Ello puede implicar los pasos de enviar datos credenciales, por ejemplo una ficha de certificación, a los terminales 1, 2 y de enviar la instrucción a los terminales 1, 2 de establecer un canal de comunicaciones "peer-to-peer" entre los terminales 1, 2. Así por ejemplo, los datos credenciales pueden incluir claves de autenticación y claves secretas para un algoritmo de encripción.

Con relación a la Fig. 2, el curso para el establecimiento dinámico de un canal de comunicaciones "peer-to-peer" entre un primer y un segundo terminal se describirá en los siguientes párrafos. Inicialmente, el primer terminal 1 y el segundo terminal 2 están conectados a través de las redes 5, 6 con la red securizada 9 por medio de canales de comunicaciones securizados 7, 8.

En el paso S1 el primer terminal 1 genera una solicitud de conexión para conectar el primer terminal 1 con el segundo terminal 2. La solicitud de conexión puede ser iniciada por un programa de aplicación instalado en el terminal 1; por ejemplo, la solicitud de conexión puede ser iniciada por un programa de cliente FTP (FTP: File Transfer Protocol), por un programa de gestión de archivos, o por cualquier otro medio. La solicitud de conexión puede estar basada en cualquier protocolo adecuado; por ejemplo, la solicitud de conexión puede estar basada en un protocolo FTP, en un protocolo SMB (SMB: Server Message Block), o en un protocolo NFS (NFS: Network File System). La solicitud de conexión puede comprender datos para recibir un archivo desde el segundo terminal 2. Típicamente, la solicitud de conexión puede comprender una dirección de fuente del primer terminal, una dirección de destino del segundo terminal, un número de puerto del segundo terminal, y una instrucción "get" para transferir un archivo desde el segundo terminal al primer terminal. Como tal, la solicitud de conexión será enviada hacia el terminal 2 por medio del interfase de red 3, el canal de comunicaciones securizado 7, la red securizada 9, el canal de comunicaciones securizado 8, y el interfase de red 4.

En el paso S2 el módulo analizador A recibe, analiza, e intercepta potencialmente la solicitud de conexión. Basado en datos contenidos en la solicitud de conexión, el módulo analizador A puede detectar que la solicitud de conexión daría lugar a la transmisión de datos desde el segundo terminal 2 a la red securizada 9 y al primer terminal 1. A raíz de tal detección, el módulo analizador puede estar configurado de tal manera que busque modos para una transmisión de datos más eficiente, dando lugar a los pasos que se describen a continuación. En la Fig. 2 el módulo analizador está vinculado al interfase de red 3. De manera equivalente, el módulo analizador A puede estar vinculado al primer terminal 1, a la red securizada 9, al interfase de red 4, al segundo terminal 2, o a cualquier otra ubicación adecuada para la recepción de una solicitud de conexión.

En el paso S3 el módulo analizador A envía al interfase de red 4 una solicitud para la recepción de parámetros de red. Además, el módulo analizador A solicita del interfase de red 3 la transmisión de sus parámetros de red. Así por ejemplo, estas solicitudes pueden estar basadas en el protocolo SNMP (SNMP: Simple Network Management Protocol) o en cualquier otro protocolo adecuado para la recepción de parámetros de red de interfases de red. Parámetros de red de interfases de red pueden comprender la dirección IP del primer y el segundo terminal 1, 2, una lista de

interfases de red disponibles (por ejemplo Ethernet, WLAN, Bluetooth, etc.), identificaciones de ISPs (ISP: Internet Service Provider), identificación de redes, disponibilidad de conexiones a dispositivos locales o remotos, etc. El paso S3 puede ser saltado si el módulo analizador A ha recibido ya de antemano parámetros de red válidos, por ejemplo si tales parámetros fueron recibidos únicamente un período de tiempo definible antes.

En el paso S4 el módulo analizador A recibe parámetros de red de los interfases de red 4, así como parámetros de red de los interfases de red 3. El paso S4 depende del paso S3, y será realizado únicamente si el paso S3 ha dado lugar a una solicitud para enviar parámetros actualizados de los interfases de red 3, 4. El paso S3 y el paso S4 pueden ser realizados enviando y recibiendo datos a través de canales de comunicaciones securizados 7 y 8.

En el paso S5 el módulo analizador A analiza los parámetros de los interfases de red 3 y 4, y busca una red 10 adecuada para establecer una conexión "peer-to-peer" entre el primer terminal 1 y el segundo terminal 2. Así por ejemplo, los parámetros del interfase de red 3 así como los parámetros del interfase de red 4 pueden indicar la disponibilidad del mismo "hotspot" WLAN. En un tal caso, la red proporcionada por el "hotspot" WLAN puede ser considerada como una adecuada red 10 para el establecimiento de una conexión "peer-to-peer" 11 entre el primer terminal 1 y el segundo terminal 2. Existe un número ilimitado de escenarios de cómo puede encontrarse una red 10 para el establecimiento de una conexión "peer-to-peer" 11. Así por ejemplo, el primer terminal 1 y el segundo terminal 2 pueden estar ubicados próximos entre sí en el mismo tren. Ambos terminales pueden ser conectados mediante un servicio GPRS (GPRS: Generalized Packet Radio Service) a una red de empresa 9. Además, ambos terminales pueden estar equipados con un interfase Bluetooth o un interfase IrDA. Basado en los parámetros de red de los terminales, el módulo analizador A puede detectar que ambos terminales se hallan dentro de alcance mutuo y entonces decidir que una red *ad-hoc* entre los terminales puede ser una red adecuada 10 para el establecimiento de una conexión "peer-to-peer" 11 entre los terminales. Además, el módulo analizador A puede detectar la disponibilidad de varias redes adecuadas para una conexión "peer-to-peer" 11 entre los terminales. Por razones de redundancia, razones de ancho de banda, o por cualquier otra razón, el módulo analizador puede también decidir el establecimiento de más de una conexión "peer-to-peer" 11 entre los terminales 1 y 2.

En el paso S6 el módulo analizador A envía una instrucción de conexión al primer y/o al segundo terminal 1, 2. La instrucción de conexión puede ser recibida y procesada por los terminales 1, 2 tal como se ilustra en la Fig. 2, o bien la instrucción de conexión puede ser directamente recibida y procesada por los interfases de red 3, 4. Una instrucción de conexión puede comprender datos para especificar un interfase de red 3, por ejemplo un interfase de red WLAN; puede comprender datos para especificar una red 10, por ejemplo una red WLAN, y puede comprender datos para especificar una conexión "peer-to-peer" 11. Los terminales 1, 2 y/o los interfases de terminales 3, 4 pueden entonces comenzar a establecer una conexión "peer-to-peer" de acuerdo con la instrucción de conexión.

Sin embargo, antes del establecimiento de una conexión "peer-to-peer" de acuerdo con la instrucción de conexión, en el paso S1 pueden proporcionarse a los interfases de red 3, 4 datos criptográficos para el establecimiento de la conexión "peer-to-peer" entre los terminales 1 y 2, tal como se ilustra en la Fig. 2, o a los terminales 1, 2. Así por ejemplo, a raíz de una solicitud enviada por los terminales 1, 2, o enviada por el módulo analizador A, una unidad central C ubicada dentro de la red securizada 9 puede generar y transmitir datos criptográficos, tales como claves de autenticación, claves de encripción, o fichas de seguridad, a los interfases de red 3, 4, o a los terminales 1, 2. A su recepción, los interfases 3 y 4, o los terminales 1, 2, pueden establecer, de acuerdo con los datos criptográficos recibidos y la instrucción de conexión, un canal de comunicaciones "peer-to-peer" 11 securizado, por ejemplo autenticado y encriptado, a través de la red 10 entre los terminales 1 y 2.

En el paso S8, por ejemplo tan pronto detecta el módulo analizador A la finalización del establecimiento del canal de comunicaciones "peer-to-peer" 11, el módulo analizador A modifica, por ejemplo, la dirección de la fuente y la dirección de destino de la solicitud de conexión de acuerdo con la recién establecida conexión "peer-to-peer", y envía al terminal 2 la solicitud de conexión modificada. Mediante una tal modificación de una solicitud de conexión el establecimiento de un canal de comunicaciones entre los terminales puede convertirse en totalmente transparente para aplicaciones o para el usuario de un terminal.

La unidad central C puede configurarse de tal manera que los canales de comunicaciones securizados 7, 8 y/o los terminales 1, 2 sean verificados en intervalos de tiempo determinables. La verificación puede incluir, por ejemplo, que paquetes de red sean enviados desde la unidad central C a los terminales 1, 2 a través de canales de comunicaciones securizados 7, 8. La unidad central C puede configurarse de modo que envíe instrucciones para interrumpir una conexión "peer-to-peer" entre los terminales 1, 2 tan pronto falle una tal verificación.

En lugar de vincular el módulo analizador A a uno de los interfases de red 3, 4 ó terminales 1, 2, el módulo analizador puede también estar vinculado a la red securizada 9. Una solicitud de conexión generada en el terminal 1 será enviada a través del canal securizado 7 a la red securizada 9. El módulo analizador A puede estar dispuesto de tal manera que la solicitud de conexión pueda ser recibida y potencialmente interceptada por el módulo analizador A. Además de los datos y parámetros arriba descritos, el módulo analizador A puede también recoger datos con respecto al estado de red de la red securizada 9. Así por ejemplo, el estado de red de la red securizada 9 puede comprender una frecuencia de colisión de paquetes de datos detectada en interfases de red definibles de la red securizada 9, por ejemplo una frecuencia de colisión detectada en routers de la red securizada 9. Cuando el módulo analizador A recibe una solicitud de conexión generada por el primer terminal, además de analizar la solicitud de conexión tal como arriba descrito, el módulo analizador puede también analizar el estado de red actual y llevar a cabo ulteriores acciones

que sean dependientes del estado de red. Así por ejemplo, el módulo analizador puede decidir enviar directamente la solicitud de conexión al segundo terminal 2 si la frecuencia de colisión de red en la red securizada 9 es baja, y por tanto no establecer una conexión "peer-to-peer" entre los terminales 1, 2. Por otra parte, si el módulo analizador detecta una elevada frecuencia de colisión en la red securizada 9, el módulo analizador puede forzar el establecimiento de un canal de comunicaciones "peer-to-peer" entre el primer y el segundo terminal incluso aunque los parámetros de red de los interfases 3, 4 ó de la red 10 indicasen que únicamente estuviera disponible una conexión "peer-to-peer" de baja velocidad entre los terminales 1, 2.

REIVINDICACIONES

1. Método para el establecimiento dinámico de un canal de comunicaciones (11) entre un primer terminal (1) y un segundo terminal (2), en que el primer terminal (1) está conectado a través de un primer canal de comunicaciones securizado (7) a una red securizada (9), y en que el segundo terminal (2) está conectado a través de un segundo canal de comunicaciones securizado (8) a la red securizada (9), **caracterizado** porque el primer terminal (1) genera una solicitud de conexión para el establecimiento de un canal de comunicaciones entre el primer y el segundo terminal (1, 2),

porque la solicitud de conexión es recibida y analizada por un módulo analizador (A),

porque los parámetros de red del primer terminal (1) y del segundo terminal (2) son recibidos y analizados por el módulo analizador (A), y

porque el módulo analizador (A), basado en el análisis de la solicitud de conexión y de los parámetros de red de los terminales, transmite una instrucción de conexión al primer y/o segundo terminal (1, 2) para el establecimiento de un canal de comunicaciones "peer-to-peer" (11) -a través de una red (10) distinta de la red securizada (9)- entre el primer terminal (1) y el segundo terminal (2).

2. Método según la reivindicación 1, **caracterizado** porque el canal de comunicaciones "peer-to-peer" (11) entre el primer terminal (1) y el segundo terminal (2) es establecido como canal de comunicaciones "peer-to-peer" securizado por medio de módulos de autenticación y/o encripción.

3. Método según la reivindicación 2, **caracterizado** porque claves de autenticación y/o encripción son proporcionadas por una unidad central (C) de la red securizada (9) a los módulos de autenticación y/o encripción.

4. Método según la reivindicación 3, **caracterizado** porque la unidad central (C) recibe parámetros sobre un estado del primer terminal (1) y/o el segundo terminal (2) en intervalos de tiempo determinables y porque un canal de comunicaciones "peer-to-peer" establecido (11) es interrumpido tan pronto como el estado del primer y/o segundo terminal (1, 2) no cumpla condiciones determinables.

5. Método según una de las reivindicaciones 1 a 4, **caracterizado** porque la solicitud de conexión generada por el primer terminal (1) es interceptada por el módulo analizador (A).

6. Método según una de las reivindicaciones 1 a 5, **caracterizado** porque el primer y segundo canal de comunicaciones securizado (7, 8) entre el primer terminal (1) y la red securizada (9) y entre el segundo terminal (2) y la red securizada (9) son establecidos empleando puntos de acceso público para la conexión de terminales a redes públicas, empleando canales de comunicaciones públicos entre las redes públicas y la red securizada, y empleando módulos criptográficos para la autenticación de los terminales (1, 2) y para la encripción de los canales de comunicaciones (7, 8) entre los terminales y la red securizada.

7. Método según una de las reivindicaciones 1 a 6, **caracterizado** porque el canal de comunicaciones "peer-to-peer" (11) entre el primer terminal (1) y el segundo terminal (2) es establecido empleando al menos una red pública.

8. Método según una de las reivindicaciones 1 a 7, **caracterizado** porque el canal de comunicaciones "peer-to-peer" (11) entre el primer terminal (1) y el segundo terminal (2) es establecido a través de una red *ad-hoc* entre el primer terminal (1) y el segundo terminal (2).

9. Sistema para el establecimiento dinámico de un canal de comunicaciones (11) entre un primer terminal (1) y un segundo terminal (2), en que el primer terminal (1) está conectado a través de un primer canal de comunicaciones securizado (7) a una red securizada (9), y en que el segundo terminal (2) está conectado a través de un segundo canal de comunicaciones securizado (8) a la red securizada (9), **caracterizado** porque el primer terminal (1) comprende medios para generar una solicitud de conexión para el establecimiento de un canal de comunicaciones entre el primer y el segundo terminal (1, 2),

porque un módulo analizador (A) comprende medios para recibir y analizar la solicitud de conexión generada por el primer terminal (1),

porque el módulo analizador (A) comprende medios para recibir y analizar parámetros de red del primer terminal (1) y del segundo terminal (2), y

porque el módulo analizador (A) comprende medios para transmitir una instrucción de conexión al primer y/o segundo terminal (1, 2) para el establecimiento de un canal de comunicaciones "peer-to-peer" (11) -a través de una red (10) distinta de la red securizada (9)- entre el primer terminal (1) y el segundo terminal (2).

10. Sistema según la reivindicación 9, **caracterizado** porque el primer terminal (1) y/o el segundo terminal (2) comprenden módulos de autenticación y/o encripción.

11. Sistema según la reivindicación 10, **caracterizado** porque la red securizada comprende una unidad central para proporcionar claves de autenticación y/o claves de encripción a los módulos de autenticación y/o encripción.

12. Sistema según la reivindicación 11, **caracterizado** porque la unidad central comprende medios para solicitar parámetros sobre un estado del primer terminal (1) y/o del segundo terminal (2) en intervalos de tiempo determinables y porque la unidad central comprende medios para interrumpir un canal de comunicaciones "peer-to-peer" establecido (11) tan pronto como el estado del primer y/o segundo terminal (1, 2) no cumpla condiciones determinables.

13. Sistema según una de las reivindicaciones 9 a 12, **caracterizado** porque el módulo analizador (A) comprende medios para interceptar la solicitud de conexión generada por el primer terminal (1).

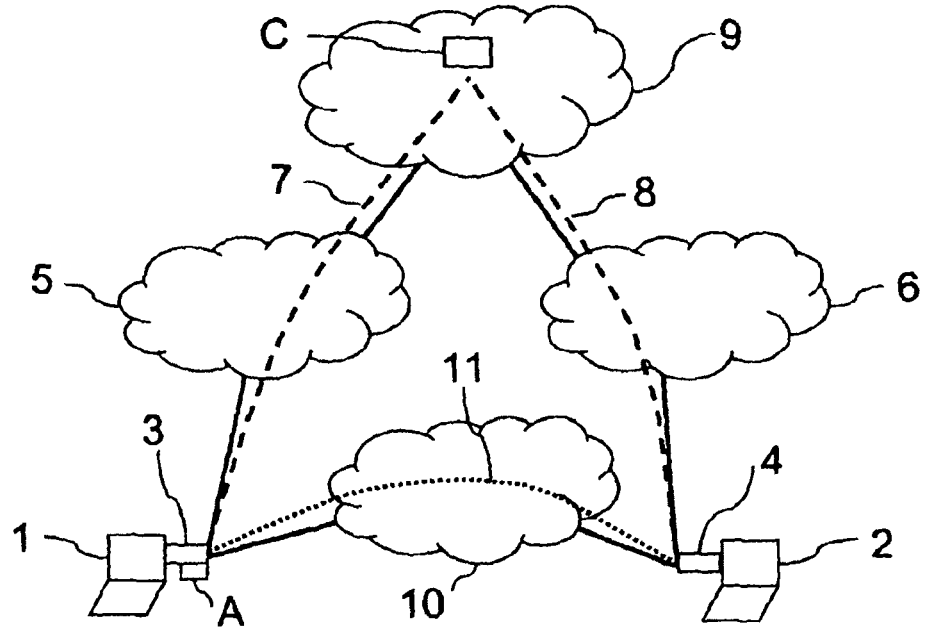

Fig. 1

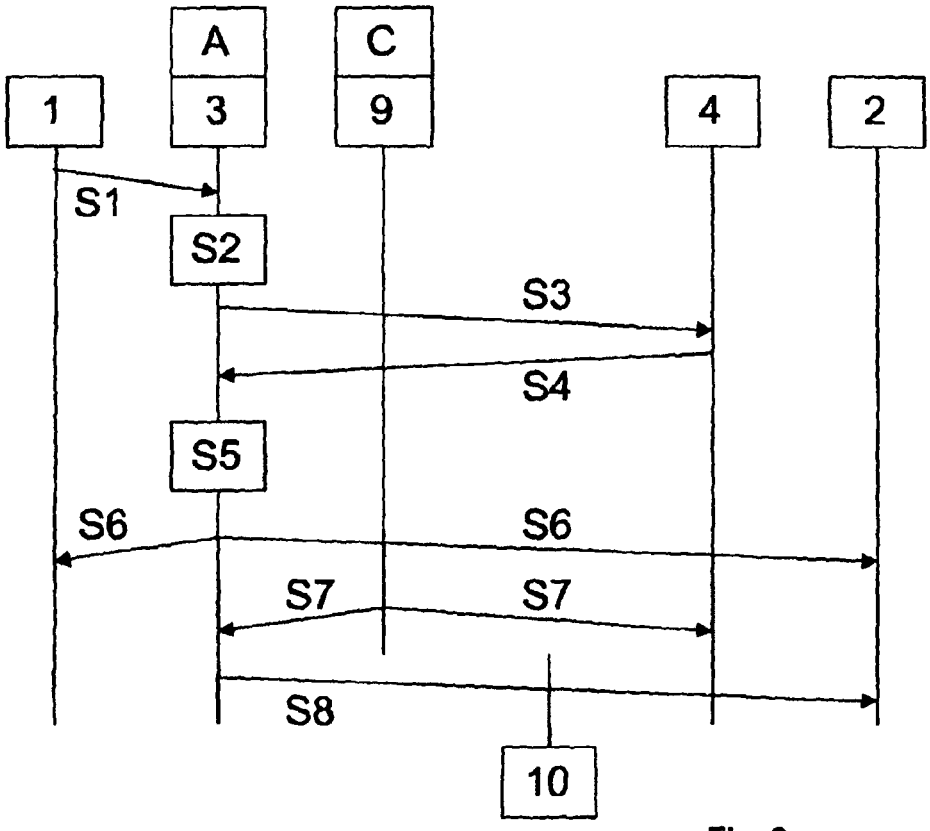

Fig. 2