



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 311 526**

51 Int. Cl.:
H04Q 7/20 (2006.01)
H04L 9/00 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Número de solicitud europea: **01944064 .3**
96 Fecha de presentación : **21.06.2001**
97 Número de publicación de la solicitud: **1316229**
97 Fecha de publicación de la solicitud: **04.06.2003**

54 Título: **Control de acceso para la comunicación en un sistema de radiocomunicación de corto alcance.**

30 Prioridad: **14.07.2000 SE 0002655**

45 Fecha de publicación de la mención BOPI:
16.02.2009

45 Fecha de la publicación del folleto de la patente:
16.02.2009

73 Titular/es: **TELIASONERA AB.**
106 63 Stockholm, SE

72 Inventor/es: **Andersin, Mikael;**
Staf, Oskar y
Strandh, Magnus

74 Agente: **Carpintero López, Mario**

ES 2 311 526 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Control de acceso para la comunicación en un sistema de radiocomunicación de corto alcance.

5 **Campo de la invención**

La invención se refiere a un procedimiento y un sistema para el control y configuración de acceso entre terminales que quieren comunicar en un sistema de radiocomunicación de corto alcance, y particularmente al control de acceso de productos Bluetooth por medio de un servidor de control de acceso.

10 **Antecedentes**

El Bluetooth es un concepto de la comunicación de radiofrecuencia de corto alcance que ha sido recibido con gran atención últimamente y que al mismo tiempo ha sido desarrollado con gran rapidez. De ser con anterioridad ejecutado mediante un consorcio cerrado con unos pocos operadores, Ericsson, Nokia y algunos otros, hoy día varios cientos de operadores están implicados en desarrollar productos dentro del campo. El Bluetooth por ejemplo se utilizará para conectar diferentes tipos de unidades entre sí. Ejemplos de ellos son:

- Computadora con teléfono móvil
- Teléfono móvil con impresora
- Teléfono móvil con manos libres portátil
- Computadora con cámara, etc.

La tecnología es utilizada también para crear pequeñas redes temporales, llamadas redes *ad hoc*. Las posibilidades son, hablando en términos generales, innumerables, y de hecho solo la imaginación limita lo que puede conseguirse con el Bluetooth.

Un aspecto importante en esta cuestión es la seguridad. Por supuesto es de gran importancia asegurar que los diferentes productos con el Bluetooth en ellos no puedan comunicar entre sí de ninguna manera. En el concepto Bluetooth esto ha sido resuelto al tener cada unidad de Bluetooth un número de identidad único BD_ADDR que se determina de acuerdo con el estándar IEEE 802. Puede decirse que se corresponde con el IMSI del GSM. En cada unidad de Bluetooth habrá también un soporte para que la unidad tenga en cuenta con qué otras unidades Bluetooth les será permitido comunicar.

El documento T. Muller, "Arquitectura de Seguridad Bluetooth, Versión 1.0" ["Bluetooth Security Architecture, Version 1.0"] 15 de Julio de 1999 trata del problema de la seguridad en los sistemas de radiocomunicación Bluetooth. Se describe un gestor de seguridad, el cual, durante el establecimiento de la conexión, comprueba si a una primera unidad se le permite tener acceso a un segundo dispositivo.

En un próximo futuro será posible predecir que habrá una gran cantidad de productos de diferentes tipos con componentes Bluetooth en ellos de forma que cada unidad tenga que ser configurada para esos componentes con los cuales serán capaces de comunicar por medio del Bluetooth. Esto puede aplicarse tanto en casa como en la compañía. Esto se traduce en un gran problema administrativo que claramente corre el riesgo de convertirse en inflexible si al mismo tiempo tiene que ser seguro.

La presente invención pretende resolver este problema.

Se han descrito diferentes sistemas y procedimientos para el control de acceso en diferentes tipos de redes de comunicación. Un ejemplo es el documento US 5,999,978 a nombre de Angal *et al.*, en el que se analiza el control de acceso en una red informática. Un servidor de acceso controla el acceso a los terminales dependiendo de la información existente en una base de datos de acceso. En el documento EP 935221 de Mitsubishi, se muestra un sistema en el cual los usuarios se autentican por medio de sensores biométricos, por ejemplo lectores de huellas dactilares, para que se les permita comunicar dentro de una red. En el documento WO 98/20646 se describe un sistema en el cual cada computadora de una red tiene una dirección IP propia, y en el que los derechos de acceso en estas computadoras están definidos en una tabla. Algunos otros documentos en el campo son WO 98/57510, JP, A, 09-130397, JP, A, 10-232811 y JP, A, 11-024978.

Ninguno de estos documentos, sin embargo, se ocupa de los problemas de los que trata la presente invención, ni se muestra ninguna solución que pueda aplicarse a estos problemas. El control de acceso dentro de las redes de corto alcance, por ejemplo Bluetooth, tiene muchos problemas. En primer lugar, la tecnología de comunicación Bluetooth está fundamentalmente dirigida a unidades portátiles. Estas son, por razones de peso y espacio, a menudo pequeñas y tienen una potencia de procesamiento, capacidad de almacenaje y consumo de potencia limitadas. En consecuencia, no se quiere cargar estos terminales con elementos tales que puedan ser manipulados por estaciones fijas. En segundo lugar, en el sistema, esto es, el Bluetooth se incluyen unidades que no tienen la posibilidad de un contacto continuo, como en el caso de estaciones móviles dentro de un sistema telefónico celular. En dicho sistema, por ejemplo el GSM,

las áreas de cobertura, las celdas, se superponen, y están definidas por las unidades de red fijas, las estaciones de base. La red fija está ahí todo el tiempo, y toda la información en ella es siempre accesible, siempre que se esté autorizado a ello. En el Bluetooth, temporalmente, se crean redes limitadas, y en dicha red normalmente no hay garantía cerca de qué capacidades dentro de la red existirán, ni qué tipo de información que esté accesible en la red, en la forma que alguien en el GSM más o menos siempre tiene contacto con un Proveedor de Servicios, SP, que proporciona los servicios de red.

Estos son algunos de los problemas que la invención pretende resolver.

10 Sumario de la invención

Con el fin de resolver los problemas anteriormente mencionados, la presente invención de acuerdo con un aspecto se refiere a un procedimiento para el control de acceso de una comunicación directa dentro de un primer sistema de radiocomunicación de corto alcance con una primera unidad con una primera identidad dentro de dicho primer sistema de radiocomunicación y una segunda unidad con una segunda identidad dentro de dicho primer sistema de radiocomunicación,

caracterizado por, en las siguientes etapas:

- la primera unidad transmite, por medio de un primer sistema de radiocomunicación, información relativa a su identidad a la segunda unidad, con la cual la primera unidad quiere comunicar;
- la segunda unidad transmite una solicitud de acceso a un servidor de control de acceso, por medio de una conexión segura sobre una portadora de un segundo sistema de comunicación, cuya solicitud de acceso incluye información relativa a dicha primera identidad y dicha segunda identidad;
- el servidor de control de acceso comprueba, en una memoria, con qué unidades dicha segunda unidad tiene derechos de acceso para comunicar dentro de dicho primer sistema de radiocomunicación;
- el servidor de control de acceso transmite la información de acceso a la segunda unidad por medio de dicha conexión segura dentro de dicho segundo sistema de comunicación, relativa al derecho de la segunda unidad de comunicar con la primera unidad dentro del primer sistema de radiocomunicación; y
- la comunicación directa es aceptada e iniciada entre la primera unidad y la segunda unidad (2) por medio de dicho primer sistema de radiocomunicación dependiendo de dicha unidad de acceso.

En una forma de realización la etapa de transmisión de la información de acceso va precedida por la etapa de almacenamiento en dicho dispositivo de control de acceso de dicha información de acceso en una memoria. La etapa de transmisión de la información de acceso a la segunda unidad se inicia en una forma de realización mediante el dispositivo del control de acceso. En otra forma de realización la etapa de transmisión de la información de acceso va precedida por la etapa de transmisión de una solicitud de acceso desde la segunda unidad hasta dicha unidad de control de acceso, solicitud de acceso que incluye información acerca de dicha primera identidad y dicha segunda identidad.

En una forma de realización preferente, dicho servidor de control de acceso es administrado/gestionado por una autoridad certificada. Dicha segunda unidad comunica en una forma de realización con el servidor de control de acceso por medio de una portadora dentro de una red de comunicación celular inalámbrica, y en una forma de realización alternativa por medio de una red de comunicación alámbrica/por cable.

De acuerdo con un segundo aspecto, la invención se refiere a un sistema de control de acceso para dirigir una comunicación entre unidades dentro de un sistema de radiocomunicación de corto alcance, que incluye

- una primera unidad dispuesta con un primer dispositivo de comunicación con una primera identidad dentro de dicho primer sistema de comunicación;
- una segunda unidad dispuesta con un segundo dispositivo de comunicación con una segunda identidad dentro de dicho primer sistema de radiocomunicación, primero y segundo dispositivos de comunicación que están dispuestos para comunicar directamente entre sí dentro de dicho primer sistema de comunicación;
- un servidor de control de acceso que incluye unos dispositivos de almacenaje que almacenan la información de acceso relativa a con qué unidades dicha segunda unidad tiene derechos de acceso para comunicar dentro de dicho primer sistema de radiocomunicación, incluyendo dicho servidor de control de acceso un dispositivo de comunicación conectado a dicho dispositivo de almacenaje e incluyendo dicha segunda unidad un cuarto dispositivo de comunicación, en el que dichos tercero y cuarto dispositivos de comunicación están dispuestos para comunicar entre sí por medio de una conexión segura dentro de un segundo sistema de comunicación, estando dicho tercer dispositivo de comunicación dispuesto para recibir una solicitud de acceso de dicho cuarto dispositivo de comunicación, solicitud de acceso que incluye dichas primera y segunda identidades, y para transmitir dicha información de acceso a dicho cuarto dispositivo de comunicación dependiendo de la solicitud de acceso.

El servidor de control de acceso de acuerdo con una forma de realización incluye unos dispositivos de procesamiento/acción conectados a dicho dispositivo de almacenaje y dicho tercer dispositivo de comunicación, dispuestos para derivar dicha información de acceso existente en dicho dispositivo de almacenaje dependiendo de dicha solicitud.

En otra forma de realización, en la que el servidor de control de acceso incluye también unos dispositivos de procesamiento/acción conectados a dichos dispositivo de almacenaje y tercer dispositivo de comunicación, dichos dispositivos de procesamiento/acción están dispuestos para derivar dicha información de acceso existente en dicho dispositivo de almacenaje y para iniciar una transmisión de la información de acceso dependiendo de parámetros preestablecidos. Dichos parámetros pueden incluir intervalos de tiempo preestablecidos de transmisión, o información acerca de la nueva información de acceso almacenada, en los cuales se lleva a cabo una transmisión, por ejemplo, en cada nueva información almacenada relativa al acceso a la segunda unidad.

Dicho segundo sistema de comunicación es en una forma de realización una red de comunicación inalámbrica celular, pero puede también incluir una red de comunicación alámbrica/por cable.

Breve descripción de los dibujos

A continuación se describirán con detalle determinadas formas de realización preferentes, con referencia al mismo tiempo al dibujo que se acompaña, en el cual:

La Figura 1 ilustra de forma esquemática unos terminales Bluetooth y un servidor de acceso de acuerdo con una forma de realización de la presente invención.

Descripción detallada de determinadas formas de realización preferentes

La idea de la invención simplemente es, por medio de portadoras diferentes, configurar y proporcionar un acceso para productos que comunican por/con Bluetooth. Dichas portadoras pueden por ejemplo ser SMS, GPRS, WAP, UMTS o http. Como sugerencia la tecnología es implementada mediante una solución de servidor donde se tiene un servidor de BCAC (Control de Acceso y Configuración Bluetooth) que comunica con productos que tienen en ellos productos Bluetooth. La característica singular es que la comunicación para asegurar los derechos de acceso se efectúa a través de una conexión segura, en contraste con la propia interfaz Bluetooth, la cual es compartida por todos los productos dentro del radio de alcance de la comunicación.

En la Figura 1 se ilustra de forma esquemática un ejemplo de una forma de realización de la invención en el que una computadora 1 detecta la existencia de un teléfono móvil 2 por medio del Bluetooth 3, y quiere comunicar con él. El teléfono móvil 2 está configurado y obtiene un control de acceso desde el servidor BCAC 4 por medio de una portadora apropiada 5, en este caso la sugerencia es un SMS. El servidor 4 transmite un mensaje Acceso Garantizado 6 que posibilita que a la unidad 2, que es el teléfono móvil, con la dirección Bluetooth x se le permita comunicar con la unidad, que es la computadora, que tiene la dirección Bluetooth y. El mensaje de Acceso Garantizado 6 puede ir precedido por una solicitud 7 procedente de la unidad 2 al servidor 4, la cual preferentemente es iniciada por el teléfono móvil 2 que ha detectado la existencia de la computadora 1 y de la dirección y. También esta solicitud 7 es transmitida a través de la conexión fija por medio de la portadora 5. La tecnología será de particular interés si el servidor BCAC 4 está controlado por una autoridad certificada como las Autoridades de Certificación de Internet.

La invención puede utilizarse en una pluralidad de situaciones. Un ejemplo se refiere a la administración del sistema. En la mayoría de los casos las compañías tienen un administrador/gestor del sistema que administra / gestiona los sistemas IT existentes en la compañía. Por medio del servidor BCAC conectado a diferentes productos informáticos, la persona en cuestión puede más fácilmente administrar el equipamiento que comunica por medio de la tecnología bluetooth. Por medio de, por ejemplo, una computadora conectada al servidor BCAC, el administrador puede decidir qué unidades que podrán comunicar entre sí, por ejemplo teléfonos móviles que pertenecen a personas que están situadas en determinado piso podrán comunicar con la impresora situada en el mismo piso.

En algunos casos puede ser de interés para las compañías permitir a los visitantes que están de visita hacer uso de su propia infraestructura interna. Un/a cliente puede, por ejemplo, querer imprimir un documento de su computadora 8 que ha traído con el/ella, en la impresora de la compañía 9, o desde la computadora 8 poder mostrar una representación por medio del proyector fijo OH instalado de la compañía. Esto puede llevarse a cabo de forma segura, dado que el cliente visitante solo tendrá acceso a una cantidad limitada del equipamiento. Además es deseable que ello se realice con una máxima flexibilidad de forma que, por ejemplo, un recepcionista no necesite estar yendo y viniendo para atender al cliente visitante. De acuerdo con la presente invención esto se obtiene mediante, por ejemplo, la conexión de la computadora 10 del/la recepcionista mediante su computadora 10 con el servidor BCAC 4, mediante lo cual el/la recepcionista atiende a que las unidades 9 que pueden ser de interés al visitante estén configuradas de forma que el visitante pueda utilizarlas. Esta configuración incluye la transmisión de la entidad BD-ADDR Bluetooth de la computadora 8 del visitante. El servidor BCAC 4 puede también estar situado con un Proveedor de Servicios, SP, en el cual la comunicación entre la compañía y el SP se lleva a cabo por medio de una conexión segura, por ejemplo una conexión IPSec.

ES 2 311 526 T3

En el futuro entonces puede ser simplemente natural proporcionar/declarar el número de identidad de los propios productos Bluetooth que uno quiere utilizar como uno hoy proporciona/declara el número de registro del coche al aparcar en el aparcamiento para visitantes.

5 La solución que se propone en la presente invención será de particular interés si el bluetooth se utiliza en entornos públicos, por ejemplo una impresora que esté situada en un lugar público de una gran ciudad/ciudad, por ejemplo en la oficina de correos o establecimiento similar. Mediante la incorporación de todos los clientes de un SP en un servidor BCAC, a todos los clientes propios se les puede ofrecer acceso automático al equipamiento que es gestionado por el servidor BCAC. Cuando se instalen más equipamientos en entornos públicos no se necesitará configurar todas las
10 unidades que comuniquen con cada equipamiento, sino que esto se llevará a cabo de forma centralidad por medio del servidor BCAC.

Se han descrito a modo de ejemplo determinadas formas de realización preferentes de la invención, pero para el experto es evidente que la solución propuesta puede modificarse dentro del concepto de acuerdo con la invención. Así
15 mismo, el experto comprenderá que la solución propuesta puede ser aplicada también a otros sistemas de comunicación de corto alcance, por ejemplo al sistema RPI (“Informática De Tráfico de Carreteras” [“Road Traffic Informatics”]), los cuales en consecuencia están amparados por el alcance de protección de la invención, alcance de protección que está solo limitado por las reivindicaciones de la patente adjuntas.

20

25

30

35

40

45

50

55

60

65

REIVINDICACIONES

1. Procedimiento para el control de acceso de comunicación directa dentro de un primer sistema de radiocomunicación de corto alcance (3) entre una primera unidad (1) con una primera identidad (y) en dicho primer sistema de radiocomunicación y una segunda unidad (2) con una segunda identidad (x) en dicho primer sistema de radiocomunicación (3),

caracterizado por las siguientes etapas:

- la primera unidad (1) transmite, por medio de dicho sistema de radiocomunicación (3), información relativa a su identidad (x) a la segunda unidad (2), con la cual quiere comunicar la primera unidad;
- la segunda unidad (2) transmite una solicitud de acceso (7) a un servidor de acceso (4), por medio de una conexión segura sobre una portadora dentro de un segundo sistema de comunicación (5), solicitud de acceso (7) que incluye información relativa a dicha primera identidad (x) y a dicha segunda identidad (y);
- el servidor de control de acceso (4) comprueba, en una memoria, con qué unidades dicha unidad (2) tiene derechos de acceso para comunicar dentro de dicho primer sistema de radiocomunicación (3);
- el servidor de control de acceso (4) transmite la información de acceso (6) a la segunda unidad (2) por medio de dicha conexión segura dentro de dicho segundo sistema de comunicación (5) relativa al derecho de la segunda unidad (2) para comunicar con la primera unidad (1) del primer sistema de radiocomunicación (3); y
- una comunicación directa es aceptada e iniciada entre la primera unidad (1) y la segunda unidad (2) por medio de dicho primer sistema de radiocomunicación (3) dependiendo de dicha información de acceso (6).

2. Procedimiento de acuerdo con la reivindicación 1, en el que dicho servidor de control de acceso es administrado/gestionado por una autoridad certificada (CA).

3. Procedimiento de acuerdo con la reivindicación 1, en el que dicha segunda unidad comunica con el servidor de control de acceso por medio de una portadora dentro de una red de comunicación celular inalámbrica.

4. Procedimiento de acuerdo con la reivindicación 1, en el que dicha segunda unidad comunica con el servidor de control de acceso por medio de una red de comunicación alámbrica/por cable.

5. Procedimiento de acuerdo con la reivindicación 1, en el que dicho sistema de radiocomunicación (3) es un sistema Bluetooth.

6. Sistema de control de acceso para una comunicación directa entre unidades dentro de un primer sistema de radiocomunicación de corto alcance (3) que incluye:

- una primera unidad (1) dispuesta con un primer dispositivo de comunicación con una primera identidad (y) dentro de dicho sistema de radiocomunicación (3);
- una segunda unidad (2) dispuesta con un segundo dispositivo de comunicación con una segunda identidad (x) dentro de dicho primer sistema de comunicación (3), primer y segundo dispositivos de comunicación que están dispuestos para comunicar directamente entre sí dentro de dicho primer sistema de radiocomunicación;
- un servidor de control de acceso (4) que incluye unos dispositivos de almacenaje que almacenan información (6) de acceso relativa a con qué unidades (1) dicha segunda unidad (2) tiene derechos de acceso para comunicar dentro de dicho primer sistema de radiocomunicación (3), incluyendo dicho servidor de control de acceso (4) un tercer dispositivo de comunicación conectado a dicho dispositivo de almacenaje e incluyendo dicha segunda unidad un cuarto dispositivo de comunicación, en el que dichos tercer y cuarto dispositivos de comunicación están dispuestos para comunicar entre sí por medio de una conexión segura dentro de un segundo sistema de comunicación (5), estando dicho tercer dispositivo de comunicación dispuesto para recibir una solicitud de acceso (7) de dicho cuarto dispositivo de comunicación, solicitud de acceso que incluye dichas primera (y) y segunda (x) identidades, y para transmitir dicha información de acceso (6) a dicho cuarto dispositivo de comunicación dependiendo de dicha solicitud de acceso.

7. Sistema de control de acceso de acuerdo con la reivindicación 6, que incluye unos dispositivos de procesamiento/acción conectados a dicho dispositivo de almacenaje y a dicho tercer dispositivo de comunicación, dispuesto para derivar dicha información de acceso existente en dicho dispositivo de almacenaje dependiendo de dicha solicitud de acceso.

ES 2 311 526 T3

8. Sistema de control de acceso de acuerdo con la reivindicación 6, que incluye unos dispositivos de procesamiento/acción conectados a dicho dispositivo de almacenaje y a dicho tercer dispositivo de comunicación, dispuestos para derivar dicha información de acceso existente en dicho dispositivo de almacenaje y para iniciar la transmisión de la información de acceso dependiendo de unos parámetros preestablecidos.

5

9. Sistema de control de acceso de acuerdo con la reivindicación 8, en el que dichos parámetros incluyen unos intervalos de tiempo preestablecidos.

10. Sistema de control de acceso de acuerdo con la reivindicación 8, en el que dichos parámetros incluyen información acerca de una nueva información de acceso almacenada.

11. Sistema de control de acceso de acuerdo con la reivindicación 6, en el que dicho segundo sistema de comunicación es una red de comunicación celular inalámbrica.

12. Sistema de control de acceso de acuerdo con la reivindicación 6, en el que dicho segundo sistema de comunicación es una red de comunicación alámbrica/por cable.

15

13. Sistema de control de acceso de acuerdo con la reivindicación 6, en el que dicho primer sistema de radiocomunicación (3) es Bluetooth.

20

25

30

35

40

45

50

55

60

65

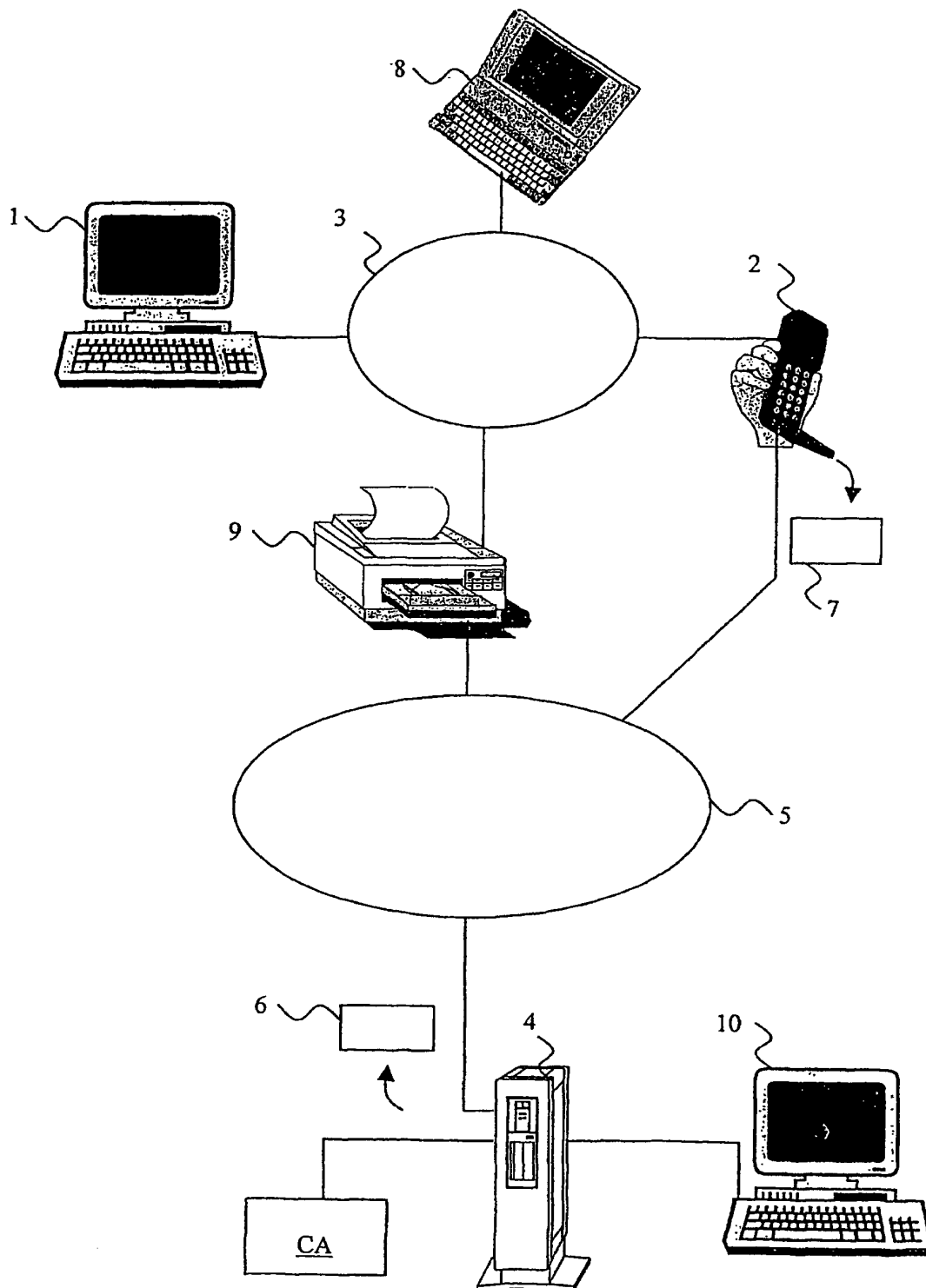


Fig. 1