(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 379 790**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07787479 .0**
(96) Fecha de presentación : **12.07.2007**
(97) Número de publicación de la solicitud: **2041923**
(97) Fecha de publicación de la solicitud: **01.04.2009**

(54) Título: **Procedimiento y disposición para la creación de redes de acceso a una red pública.**

(30) Prioridad: **14.07.2006 DE 10 2006 033 830**

(45) Fecha de publicación de la mención BOPI:
03.05.2012

(45) Fecha de la publicación del folleto de la patente:
03.05.2012

(73) Titular/es: **CUCULUS GmbH**
Ehrenbergstrasse 11
98693 Ilmenau, DE

(72) Inventor/es: **Kärst, Holger;**
Böringer, René y
Scharfe, Gunnar

(74) Agente/Representante:
Blanco Jiménez, Araceli

DESCRIPCIÓN

Procedimiento y disposición para la creación de redes de acceso a una red pública.

La presente invención se refiere a un procedimiento y una disposición para la creación de redes de acceso a una red pública. Con ella se realizan redes inalámbricas flexibles y rentables en regiones geográficamente amplias (ciudades, polígonos industriales) mediante el uso y la administración común de una infraestructura de red existente y con los mismos derechos repartidos entre varios gestores (p.ej. proveedores).

En la actualidad existen diferentes procedimientos y disposiciones para la construcción y la operación de redes de acceso, como p.ej. los de la WO 2006/021784 A1. Las redes de acceso conectan terminales con capacidad de red (teléfonos móviles, PDAs, ordenadores portátiles, ordenadores de sobremesa) o redes locales (p.ej. redes particulares) de forma inalámbrica o con cables entre sí o con una red global (p.ej. pública).

La US 2005/0237985 A1 también describe un procedimiento similar en el que, en la formación de una red de acceso, los recursos se asignan según los derechos definidos para cada proveedor.

El procedimiento tradicional para la construcción y la operación de redes de acceso puede denominarse "proceso basado en el proveedor". Un proveedor, por ejemplo, ofrece a los terminales con capacidad de red o a las redes locales (p.ej. particulares) unos puntos de acceso (en su conjunto: red de acceso) para una red global (p.ej. pública) o para servicios, respectivamente, de una red global (p.ej. pública) a cambio del pago de una tarifa (figura 1). El proveedor mismo construye e instala los puntos de acceso. Por lo general, también sólo el proveedor ofrece la puesta a disposición, la gestión y el servicio técnico para los puntos de acceso. De esta manera, un proveedor puede garantizar a sus clientes uniformidad de la gestión de servicios, la compatibilidad de los puntos de acceso de su red y una alta calidad de servicio técnico. Sin embargo, el proveedor tiene que correr sólo con los costes de inversión relativamente altos, como p.ej. la construcción y la instalación de la infraestructura de red (de ahora en adelante denominada también infraestructura), la adquisición de las instalaciones para cada punto de acceso y los costes elevados de operación, como p.ej. por el alquiler de las instalaciones, costes de mantenimiento y costes de energía de los puntos de acceso. Por esta razón, las arquitecturas basadas en los proveedores sólo resultan rentables económicamente cuando sean utilizadas durante un período de tiempo prolongado sin sufrir alteraciones.

Para poder disminuir los altos costes de inversión y operación para los proveedores de una red de acceso, y, al mismo tiempo, incrementar la flexibilidad del proveedor, existe un alto interés económico en nuevos procedimientos en los que diferentes partes (30, 31) (p.ej. varios proveedores o una persona particular y un proveedor) usen una infraestructura de forma múltiple. Con estos procedimientos, por ejemplo, sería posible que una infraestructura ofreciera varias redes de acceso de distintos proveedores o liberar infraestructuras ya existentes pertenecientes a un dueño para poner a disposición unas redes de acceso a través de terceros o, respectivamente, para extender la puesta a disposición de unas redes de acceso a través de terceros. Ya se han desarrollado algunos procedimientos y arquitecturas que se basan en el principio del uso común de una infraestructura por varias partes (30, 31).

En todos los procedimientos y disposiciones conocidos hasta ahora, siempre existe un "supervisor" (en el estado de la técnica también denominado como parte Root) que posee el control absoluto sobre la infraestructura de uso común. Un supervisor posee los privilegios que le permiten, de forma arbitraria, y teóricamente sin necesidad de consultar a las demás partes (30, 31) de la infraestructura de uso común, la realización de modificaciones en la infraestructura, que también pueden tener efectos sobre la infraestructura de las partes (30, 31). Aquí se puede clasificar dos principios distintos. De ahora en adelante estos dos principios se denominarán "principio de control por el gestor" y "principio de control por el dueño".

El "principio de control por el gestor" delimita todos los procedimientos y disposiciones en los que el control de la infraestructura es completamente del gestor (p.ej. proveedor) de la infraestructura (la infraestructura propia del gestor y también la infraestructura cuyo dueño son terceros pero que son administradas por un gestor). El control puede comprender parámetros económicos (p.ej. contabilidad y facturación de los usuarios (30, 31)) y posibilidades de configuración de los parámetros técnicos (p.ej. administración QoS y de ancho de banda, administración de las opciones de red). A los dueños que ceden su infraestructura parcial o totalmente para el uso común se le retira la autoridad de administración sobre su infraestructura por completo para transferirla al gestor. El gestor se vuelve supervisor. Los procedimientos tradicionales basados en el proveedor pueden subordinarse claramente bajo el "principio de control por el gestor".

El "principio de control por el dueño" comprende todos los procedimientos y disposiciones en los que el dueño posee el control absoluto sobre su propia infraestructura y sobre la propia infraestructura cedida a terceros para su uso. Los terceros pueden usar esta infraestructura cedida para sus propios fines, sin embargo, no poseen ninguna influencia sobre los ajustes de los parámetros de esta infraestructura. El dueño sigue siendo supervisor. El "principio de control por el dueño" se refleja en los procedimientos basados en comunidades.

Los procedimientos basados en comunidades son todavía y hasta hoy en día muy nuevos. En una comunidad, los términos proveedor y cliente se fusionan entre sí. Los participantes en la comunidad ofrecen su propia infraestructura (p.ej. puntos de acceso a otras redes) o servicios (actúan como proveedores), pero también utilizan infraestructuras y servicios ofrecidos por otros participantes de la comunidad (actúan como clientes) (figura 2). Los costes de inversión

y de operación se subvienen en común por todos los participantes. Una comunidad, por esta razón, puede ofrecer a sus participantes un uso económico o incluso gratis de la infraestructura puesta a disposición o de los servicios puestos a disposición, respectivamente, y es flexible a la hora de la integración de nuevas tecnologías. En un procedimiento basado en una comunidad, los acuerdos sobre las modificaciones se toman de forma democrática, sin embargo, los participantes de la comunidad no están obligados a implementar dichas alteraciones. La distribución de la responsabilidad por la red que esto conlleva tiene como desventaja que apenas se puede gestionar los servicios de forma uniforme y óptima. Los diferentes elementos de la infraestructura generan incompatibilidades. La fiabilidad de la infraestructura y de los servicios ofrecidos es muy baja. La calidad del servicio técnico tiene un nivel muy bajo o incluso inexistente.

Como cada participante de la comunidad también puede ser proveedor de servicios, por ejemplo ser proveedor de un punto de acceso público a Internet para la comunidad, este participante puede considerarse, en el sentido legal y según las leyes de un país, un proveedor. Por consiguiente, este participante debe cumplir con las normas reguladoras y legales aplicables a los proveedores. Sin embargo, un participante que en las comunidades en la mayoría de los casos es una persona particular, corre un riesgo elevado. Por ejemplo, podría tener que hacerse responsable de las actividades realizadas por otros participantes de la comunidad usando su punto de acceso público cedido. O el participante tiene que cumplir todas las normas reguladoras que se aplican para proveedores y, por consiguiente, debe ofrecer, por ejemplo, interfaces de acceso para autoridades oficiales del país en su punto de acceso.

El "principio de control por el gestor" y el "principio de control por el dueño" presuponen que entre el supervisor (gestor o dueño) y las otras partes de la infraestructura de uso común exista una relación de confianza absoluta. Todas las partes (30, 31) de la infraestructura común dependen por completo de los acuerdos del supervisor y están limitados al uso de las tecnologías y servicios que el supervisor defina. Esta relación de confianza entre el supervisor y las partes de una infraestructura de uso común necesaria para ambos principios, en la aplicación efectiva no es nada real. Por esta razón, hasta la actualidad no existen redes de acceso comercial con una infraestructura construida para la administración común por varias partes.

El objetivo de la presente invención, por consiguiente, es, por un lado, la concentración de las ventajas del "principio de control por el gestor" y del "principio de control por el dueño" y, por el otro lado, la eliminación de un supervisor hasta ahora imprescindible para ofrecer un procedimiento y una disposición para la creación de redes de acceso a una red pública que se base en una gestión común de infraestructuras de cualquier dueño y por varias partes. Aquí, esta disposición o procedimiento, respectivamente, cumplen además con las condiciones técnicas de seguridad que posibilitan la puesta a disposición de unos servicios comparables con los servicios de las redes de telecomunicación de la actualidad a través de infraestructuras de uso común. Además, aparte de la división del ancho de banda de una conexión de banda ancha (p.ej. conexión WAN) de una infraestructura también deberá ser posible una división real de recursos de los recursos del sistema de la infraestructura, por ejemplo, procesador, RAM, caché y otras interfaces.

Según la invención, este objetivo se alcanza, por un lado, con un procedimiento según la enseñanza de la reivindicación 1 y, por el otro lado, con una disposición según las características de la reivindicación 11, siendo las reivindicaciones dependientes otras formas de realización preferidas de la enseñanza según la invención.

El procedimiento según la invención (en lo sucesivo denominado procedimiento basado en Cuckoo) concentra, por un lado, las ventajas del "principio de control por el gestor" y del "principio de control por el dueño" sin las desventajas de cada uno y elimina, por el otro lado, el supervisor hasta ahora imprescindible. Con la invención es posible, por primera vez, que varias partes gestionen de forma común una infraestructura teniendo en cuenta, al mismo tiempo, los requisitos técnicos de la seguridad. Entre las partes no tiene por qué existir una relación de confianza.

La relación de confianza se genera indirectamente mediante el procedimiento mostrado en esta invención o por una disposición como la aquí descrita, respectivamente.

Los dueños de la infraestructura pueden poner a disposición los derechos de uso de los recursos (6, 7) de su infraestructura (anchos de banda de las interfaces de red, uso de CPU, uso de memoria, entre otros) para las demás partes (30, 31). Para ello, los derechos de uso puestos a disposición se encapsulan en un entorno de usuario independiente y flexible (4) mientras que los derechos de uso que no son puestos a disposición se quedan en el entorno de usuario encapsulado del dueño (3). Por consiguiente, la infraestructura contiene por lo menos dos entornos de usuario (3, 4) a los que cada parte correspondiente (30, 31) obtiene el acceso.

Las modificaciones que afectan a los entornos de usuario (3, 4) de varias partes (30, 31) de la infraestructura con uso común o los recursos, respectivamente, que no están asignados directamente a un entorno de usuario (8), es decir, que superan los derechos de uso de un entorno de usuario (3, 4), sólo podrán implementarse a través de un proceso de negociación después de que todas las partes (30, 31) hayan tomado una decisión común. Un proceso de negociación se define porque las partes (30, 31) en este proceso llegan, mediante procedimientos de negociación que se determinan según la disposición o según el procedimiento, respectivamente, de manera común a una decisión sobre las modificaciones de la infraestructura de uso común.

La disposición según la invención o el procedimiento según la invención, respectivamente, contienen, para ello, una unidad neutral con respecto a las partes automática -el entorno básico (5)- que controla el proceso de negociación común y supervisa el cumplimiento de las opciones negociadas. No existe, por consiguiente, ningún supervisor en el sentido clásico de alguien que posee el control absoluto sobre la infraestructura de uso común. Sin embargo, cada

parte (30, 31) puede configurar, dentro del marco de las opciones negociadas, su propio entorno de usuario (3, 4) delimitado, por ejemplo, instalar software, hacer configuraciones y proporcionar cualquier servicio (p.ej. servicios como la puesta a disposición de accesos a la red o servicios de aplicaciones como la telefonía o IPTV). Para cada parte (30, 31) su entorno de usuario (3, 4) lógico se muestra como si se tratara de una infraestructura física completamente independiente que tan sólo se usa por la parte mencionada (30, 31). Mediante la división de los derechos de uso en diferentes entornos de usuario (3, 4), el proceso basado en Cuckoo, por ejemplo, permite la construcción de redes de acceso a una red pública con una infraestructura utilizada en común por varias partes (30, 31), en el que cada red de acceso puede ofrecer las características de las redes de proveedor tradicionales. Estas características son una gestión de servicios uniforme, la compatibilidad de los puntos de acceso y una alta calidad de servicio técnico por parte del suministrador del servicio (p.ej. el proveedor) para el usuario final.

Por consiguiente, con la ayuda de la disposición según la invención o el procedimiento según la invención, respectivamente, varias partes (30, 31) pueden operar paralelamente varias redes de acceso independientes a través de una única infraestructura. Los costes de inversión y de operación se distribuyen entre las partes (30, 31) (p.ej. dueños, proveedores). Cada dueño se responsabiliza de la instalación y el mantenimiento de su infraestructura, sin embargo, no de la administración de los recursos (6, 7, 8) o participaciones de recursos (6, 7, 8) de la infraestructura, cuyos derechos de uso habría cedido.

La ventaja de esta solución según la invención puede resumirse de la siguiente forma:

- El supervisor de una infraestructura hasta ahora siempre presente se elimina. Las partes (30, 31) que usan una infraestructura en común, tienen los mismos derechos entre sí y pueden efectuar, sólo por acuerdos mutuos, modificaciones en la infraestructura y en la división de los derechos de uso de los recursos (6, 7, 8) o de las participaciones de recursos (6, 7, 8) de la infraestructura. En cambio, una unidad (5) neutral con respecto a las partes automática controla el proceso de negociación y supervisa los ajustes negociados de forma común para la infraestructura.

- Una asignación real de los derechos de uso de los recursos (6, 7, 8) para las distintas partes (30, 31) de la infraestructura no sólo es posible para el ancho de banda de la conexión inalámbrica o con cables, respectivamente (no sólo una partición de las redes en distintas redes virtuales VLAN), sino que también es posible, entre otras cosas, para interfaces, procesadores, sistemas de archivos, caché, RAM y otros medios de almacenamiento (discos duros, memorias flash).

- Cada parte (30, 31) con su entorno de usuario propio (3, 4) puede configurar su entorno libremente, por ejemplo, puede instalar cualquier servicio, herramienta y software, y, al mismo tiempo, se asegura que los otros entornos de usuario (3, 4) no se alteren por ello de ningún modo.

- Cada entorno de usuario (3, 4) se presenta, a pesar de la infraestructura de uso común, para cada parte (30, 31) de tal manera como si la infraestructura se usara única e independientemente por este parte (30, 31).

- Los derechos de uso, que están encapsulados en un entorno de usuario (3, 4) de una parte (30, 31) especifican las posibilidades de acceso a los recursos (6, 7, 8) o las participaciones de recursos (6, 7, 8) de una infraestructura usada en común por varias partes (30, 31) para dicha parte (30, 31). Así, se garantiza a la parte (30, 31), que es la única con acceso a estas participaciones de recursos (6, 7, 8) para que esta parte (30, 31) pueda planificar de forma precisa el uso de los recursos (6, 7, 8) (p.ej. los proveedores pueden garantizar a sus clientes finales una disponibilidad de los servicios).

- Las distintas redes de acceso cuya infraestructura se usa y se gestiona en común por varias partes (30, 31) pueden asegurarse mediante selección libre por cada parte correspondiente (30, 31) y con distintos mecanismos de seguridad.

- Para dividir y proteger los derechos de uso de los recursos (6, 7, 8) de la infraestructura encapsulada en entornos de usuario (3, 4), ya no es posible un acceso o una manipulación del tráfico de la red de los otros entornos.

- Además, se puede prescindir de los elementos adicionales de red (p.ej. router, servidor o switches) que efectúan, en los procedimientos y sistemas hasta ahora conocidos, la división de los corrientes de datos en una infraestructura de uso común entre varias partes (30, 31).

- No se requieren modificaciones en los terminales que usan las redes de acceso que se basan en la infraestructura de uso común. Los proveedores pueden trasladar servicios de su red principal a los puntos de acceso y, de esta manera, son mucho más flexibles en la puesta a disposición de los servicios y la configuración de sus redes.

Se deducen otros detalles de la invención de la siguiente parte descriptiva en la que la invención se explica más detalladamente con referencia a las ilustraciones adjuntas. Las figuras muestran:

La figura 1 el principio de una disposición basada en el proveedor (separación de la infraestructura de redes particulares y públicas con puntos de conexión entre las redes particulares y públicas según el estado de la técnica).

La figura 2 el principio de una disposición basada en una comunidad (la persona C ofrece a la comunidad un punto de acceso a una red pública según el estado de la técnica).

La figura 3 el principio de la disposición basada en Cuckoo (integración de una infraestructura particular en una red pública - la persona C no ha cedido sus recursos (6, 7, 8)).

La figura 4 el principio de un "principio de control por el dueño" según el estado de la técnica.

La figura 5 el principio de un "principio de control por el gestor" según el estado de la técnica.

La figura 6 el principio de una administración basada en Cuckoo.

La figura 7 la disposición basada en Cuckoo, realizada como Cuckoo Access Point (CAP) en el ejemplo de una red WLAN pública de un proveedor de servicio y una red particular de una persona.

La figura 8 un punto de acceso conocido del estado de la técnica.

La figura 9 un punto de acceso Cuckoo para dos partes (30, 31) A y B.

La figura 10 muestra una definición de interfaz del CAP con el ejemplo de dos partes (30, 31) A y B.

La figura 11 muestra una gestión controlada por el estado de los recursos repartidos (6, 7, 8).

La figura 12 la ilustración técnica de la disposición.

En lo sucesivo se hará una distinción entre personas y proveedores de servicios.

El término persona se utiliza como sinónimo de persona natural o jurídica (p.ej. una empresa). Una persona se caracteriza por ser propietario de una infraestructura con por lo menos un punto de acceso para el acceso a una red y una conexión a otra red (p.ej. una red pública, Internet). Por lo general, una persona utiliza la infraestructura para sus propios fines. Una persona no se esfuerza en ofrecer servicios con acceso por terceros.

Un proveedor de servicios utiliza la infraestructura de una o varias personas y ofrece sus propios servicios, como, por ejemplo, la telefonía o servicios de terceros a través de esta infraestructura.

Como partes (30, 31) se denominan todas aquellas personas y proveedores de servicios que usan una infraestructura en común como la del procedimiento según la invención o la disposición según la invención, respectivamente.

La siguiente forma de realización sirve únicamente para el mejor entendimiento de la invención y no la limita de ningún modo.

Cada vez más seres humanos y empresas (personas) poseen una infraestructura en forma de un acceso de banda ancha y una red particular, local, inalámbrica, p.ej. WLAN, en la que los recursos existentes (6, 7, 8) de cada acceso de banda ancha y de las redes particulares, locales, inalámbricas no se aprovechan del todo porque la necesidad particular de las personas no lo requiere.

Por otro lado, los proveedores de telefonía móvil y otras empresas (proveedores de servicios) cada vez se esfuerzan más para establecer una red basada en las ondas de radio con cobertura ininterrumpida que proporcionen velocidades de transmisión de datos muy altas y además un nuevo tipo de servicios (como p.ej. una red pública WLAN). Como las células de radioemisión en redes inalámbricas basadas en WLAN son pequeñas (con un diámetro máximo de 100 m), son necesarios muchos puntos de acceso WLAN para una cobertura de red por región, como p.ej. para toda una ciudad o un polígono industrial. Todo esto genera altos gastos económicos.

El núcleo de la invención se basa en el uso de los recursos no usados (6, 7, 8) de las infraestructuras de personas por proveedores de servicios para la puesta a disposición de servicios. De esta manera, se puede establecer en un tiempo muy corto y con muy pocos costes de instalación y de operación repartidos una red WLAN con cobertura completa para una región entera. Las personas ofrecen sus infraestructuras a los proveedores de servicios a cambio de una compensación. Los proveedores de servicio pueden aprovechar las capacidades de los accesos de banda ancha o de los recursos (6, 7, 8), respectivamente, puestas a disposición para ellos para ofrecer a sus clientes en estos sitios de los puntos de acceso un acceso inalámbrico a Internet (p.ej. células WLAN públicas) o a otros servicios, como p.ej. telefonía, transmisión de vídeo o servicios de información a través de WLAN. Los puntos de acceso, de esta forma, forman parte de la red particular local de la persona y, paralelamente, de la red pública del proveedor de servicio (figura 7). Con el procedimiento basado en Cuckoo se realiza un novedoso procedimiento para el reparto de los accesos a la red (por ejemplo, acceso a través de radioemisión, acceso por banda ancha) y los recursos (6, 7, 8) (por ejemplo, los recursos de los equipos de un punto de acceso de una red (Access Point)) entre las personas y los proveedores de servicio.

Una persona posee una infraestructura que consiste en por lo menos un acceso a una red (p.ej. red particular local) y un acceso a través de una conexión de banda ancha a otra red (p.ej. red pública, Internet). El acceso, entre otras cosas, puede realizarse mediante un punto de acceso. El punto de acceso puede contener uno o varios módulos de radioemisión para la puesta a disposición de una o varias redes inalámbricas. Dichos módulos de radioemisión pueden soportar redes inalámbricas de cualquier tecnología actual o futura y estándares como WLAN, WIMAX, UMTS, CDMA-2000, WiBRO, GSM, Bluetooth. La conexión de banda ancha puede realizarse mediante tecnologías inalámbricas o con cables, por ejemplo mediante ADSL, SDSL, VDSL, WIMAX, WLAN, UMTS, WiBRO. La persona es responsable de la puesta a disposición del sitio de la infraestructura, de la alimentación eléctrica de la infraestructura, de la conexión a red de la infraestructura y el mantenimiento y cuidado de la infraestructura. Si la propia persona tan solo utiliza su infraestructura parcialmente, esta persona puede ofrecer las partes no utilizadas de su infraestructura a uno o varios proveedores de su elección para que disponga de ella de forma libre, en la que la infraestructura ofrecida por una persona puede tener varios grados de interés porque ésta depende de la oferta de infraestructuras en el entorno cercano geográfico, la demanda de infraestructuras y de los acuerdos estratégicos y tácticas de un proveedor de servicios. La persona puede utilizar las partes de la infraestructura no cedidas para sus propios fines y usarlas de forma libre. El uso exclusivo de la parte no cedida de la infraestructura está garantizado a la persona.

La persona negocia con uno o varios proveedores de servicio potenciales un derecho de uso de su infraestructura propia a ceder a los potenciales proveedores de servicio. Los derechos de uso pueden establecerse, por ejemplo, en forma de acuerdos sobre el nivel de servicio (SLA). La persona cede, al firmar el contrato, la parte negociada de la infraestructura a uno o varios proveedores de servicio. Si las condiciones en el marco legal lo permiten (las condiciones de contrato entre la persona y el proveedor de servicio), la persona puede recuperar las partes cedidas de la infraestructura para utilizarlas para fines propios o para cederlas a otros proveedores de servicio.

La persona recibe una recompensa por los derechos de uso cedidos del proveedor de servicios o los proveedores de servicio, respectivamente. Esta recompensa puede ser de diferentes formas, por ejemplo, una compensación continua (tarifa por minuto de uso o tarifa por cantidad de información trasmitida (p.ej. paquetes de red) a través de la infraestructura cedida) o una compensación única (la infraestructura se financia total o parcialmente por el proveedor de servicio o éste ofrece el servicio a bajo coste o a ningún coste, o a una tarifa base a la persona).

Los proveedores de servicios pueden seleccionar la infraestructura ofrecida por las personas de forma flexible para su propio uso. Las redes de los proveedores de servicios, de esta manera, pueden adaptarse de forma rápida y eficiente a las modificaciones del entorno a través de la integración y también la eliminación de las partes de infraestructura de distintas personas. Las modificaciones del entorno, en este caso, describen todas las modificaciones externas e internas de red que tienen un impacto sobre la red, por ejemplo, sobre el funcionamiento y la ocupación de la red (p.ej. por modificaciones del comportamiento del usuario de los clientes finales o por un cambio de estrategia de los proveedores de servicio). Un proveedor de servicio con un derecho de uso cedido de una parte de una infraestructura o que él hubiera elegido (negociación contractual con la persona dueño de la infraestructura) puede utilizar esta parte de infraestructura para sus propios fines o fines de terceros de forma exclusiva. El uso exclusivo de esta parte de infraestructura se garantiza al proveedor de servicios.

La flexibilidad de la construcción de la red con partes de infraestructura de distintas personas y la posibilidad de la libre configuración de las partes de infraestructura, por un lado, disminuye los costes para la construcción y la operación de redes y, por el otro lado, incrementa la fuerza innovadora del proveedor de servicios. Las partes de infraestructura de una o varias personas que se han cedido al proveedor de servicio, se gestionan únicamente por el proveedor de servicios. El proveedor de servicios es el contacto central para sus clientes finales y abarca por completo las funciones del servicio técnico de todas las partes de la infraestructura gestionadas por él. De este modo, se puede garantizar a los clientes finales (los clientes del proveedor del servicio) la disponibilidad de los servicios (p.ej. acceso a Internet, telefonía) y existe un contacto central para el servicio técnico.

Sin embargo, ninguna parte (30, 31) (persona, proveedor de servicios) tiene el permiso (como se define en el contrato) o la posibilidad (separación técnica) de acceder a los datos (datos de contabilidad, autentificación, configuración u otros datos), a las unidades de datos (archivos y otros objetos o contenedores con datos) y a las partes de infraestructura de las otras partes (30, 31) de una infraestructura con uso común. El procedimiento basado en Cuckoo ofrece los mecanismos necesarios de seguridad para asegurar los datos, las unidades de datos y las partes de la infraestructura entre los proveedores de servicio y las personas mediante el encapsulado de los datos y unidades de datos y los derechos de acceso a partes de la infraestructura en los correspondientes entornos de usuario (3, 4). Las partes (30, 31) tienen los mismos derechos. Solo se pueden cambiar las condiciones de contrato o terminar contratos a través de acuerdos mutuos. Las infracciones de contrato se detectan, observan y se alegan judicialmente por todas las partes (30, 31) mediante mecanismos de monitorización y señalización de la disposición. La realización técnica del procedimiento basado en Cuckoo garantiza los derechos por igual e impide la infracción unilateral, por ejemplo, las modificaciones unilaterales de la infraestructura o las modificaciones unilaterales de la distribución predefinida de las partes de una infraestructura. No existe ningún “supervisor” que pueda revocar o alterar las limitaciones/distribuciones negociadas en común de una infraestructura de uso común.

El procedimiento basado en Cuckoo puede integrarse, en cumplimiento de las condiciones del marco legal, en redes públicas de telecomunicación y con los requisitos de seguridad de las personas y proveedores de servicio, simplemente al implementarlas en las redes ya existentes. El procedimiento basado en Cuckoo ofrece una fiabilidad suficiente para establecer un uso común de las infraestructuras por varias partes (30, 31) en la práctica. Con este procedimiento,

el uso exclusivo de cada parte de infraestructura de todas las partes (30, 31) se define precisamente por contrato y se garantiza técnicamente. El procedimiento basado en Cuckoo facilita de forma significativa la aceleración de la conquista de nuevos mercados, la reconfiguración de mercados existentes y la introducción de nuevos servicios y tecnologías.

A continuación se describe más detalladamente una posible realización técnica de la disposición basada en Cuckoo en forma de punto de acceso Cuckoo (CAP). La descripción de esta forma de realización sirve únicamente para el mejor entendimiento de la invención y no la limita de ningún modo. Particularmente, también se puede pensar en otras posibilidades de realización según la invención que, por lo general, se consideran abarcadas por la invención.

Los recursos (6, 7, 8) de un CAP de aquí en adelante se refieren a los componentes de hardware y software de un CAP. Así, un CAP comprende por lo menos los siguientes recursos (6, 7, 8):

- Soporte de una o varias interfaces de red inalámbricas o con cables (ADSL, SDLS, VDSL, WLAN, WIMAX, WiBRO, Bluetooth, UMTS, u otros) para una red pública y/o para una red particular.

- Soporte de una o varias interfaces de red inalámbricas con la misma o distintas tecnologías inalámbricas (WLAN, WIMAX, UMTS, GSM, WiBRO) con la posibilidad de una gestión dinámica de la configuración por radioemisión para la puesta a disposición de una o varias redes de acceso(s).

- Hardware básico (procesador, memoria, interfaz input-output).

- Unidades de software y hardware básicas para la realización técnica del procedimiento descrito (entorno básico (5), entorno de usuario (3, 4)), estando cada de estas unidades compuesta por diferentes módulos (72, 73, 74, 75, 76, 77, 79, 80, 81, 82).

- Sistema operativo.

- Sistema de archivos.

Un CAP puede realizarse como unidad en un dispositivo pero también puede estar distribuido en varios dispositivos. Así, un dispositivo describe una unidad de función cerrada con recursos limitados (6, 7, 8) e interfaces definidas.

Los recursos (6, 7, 8) de un CAP pueden usarse exclusivamente por una parte (30, 31) o por varias partes (30, 31) parcial o independientemente de cada parte, para poder operar con estos recursos (6, 7, 8) un punto de acceso a una red.

Para la totalidad de los derechos de uso de los recursos (6, 7, 8) o participaciones de recursos (6, 7, 8), datos (datos de contabilidad, autentificación, configuración u otros datos) y unidades de datos (archivos u otros objetos o contenedores con datos) de un CAP se utiliza el término “entorno”.

El CAP promueve, en una ampliación, las funciones que permiten que una o varias partes (30, 31) usen los recursos (6, 7, 8) del CAP de forma independiente, según los derechos de uso definidos por el contrato, arbitraria, total o parcialmente. Los derechos de uso negociados entre las partes (30, 31), por ejemplo en forma de acuerdos sobre el nivel de servicio, se reflejan técnicamente en un reglamento predefinido (78), como por ejemplo, en cláusulas, que predeterminan el acceso a los recursos (6, 7, 8) del CAP para todas las partes (30, 31) del CAP de forma precisa. Si los recursos (6, 7, 8) de un CAP se usan por varias partes (30, 31), los recursos (6, 7, 8) pueden repartirse entre las partes (30, 31) de forma lógica (p.ej. mediante la virtualización de los recursos (6, 7, 8)), por hardware (p.ej. existen los mismos componentes de hardware varias veces) o mediante la combinación de los dos. Los derechos de uso de los recursos (6, 7, 8), los datos, unidades de datos y funciones de un parte (30, 31) se encapsulan para las partes (30, 31) en entornos de usuario (3, 4) Los derechos de uso encapsulados en un entorno de usuario (3, 4) garantizan a la correspondiente parte (30, 31) el acceso exclusivo a los recursos (6, 7) especificados por los derechos de uso o a las participaciones de recursos (6, 7). Técnicamente se puede asegurar que ninguna parte (30, 31) pueda acceder a los recursos (6, 7, 8), los datos y unidades de datos de cualquier otra parte (30, 31) del CAP, ni penetrar a los entornos de las otras partes (30, 31).

Los hasta ahora conocidos puntos de acceso disponen de un entorno (1) que permite exclusivamente a una parte llevar a cabo configuraciones en el punto de acceso y controlar los recursos (2) de los puntos de acceso (figura 8). De esta manera, esta parte es el supervisor del punto de acceso. El punto de acceso Cuckoo según la invención amplia este principio mediante la divisibilidad del entorno en varias partes (figura 9) y la eliminación del supervisor. Así, la división no se limita sólo al ancho de banda de la conexión a la red inalámbrica (p.ej. mediante la puesta a disposición de varias redes inalámbricas virtuales mediante la emisión de varios ESSID) o con cables (mediante tecnologías VLAN y mecanismos QoS), sino también se pueden dividir los otros recursos (6, 7, 8), p.ej. interfaces, volúmenes de almacenamiento y capacidades de la CPU. En principio, el entorno (1) de los puntos de acceso actualmente conocidos se subdivide en el punto de acceso Cuckoo en un entorno básico (5) y por lo menos uno o también varios entornos de usuario (3, 4). Todas las funciones para encontrar los acuerdos y gestionar los recursos (6, 7, 8) que se refieren a todos los entornos de usuario (3, 4) de un CAP, se encapsulan en el entorno básico (5).

Así, el entorno básico (5) comprende por lo menos un reglamento (78), una unidad de seguridad (79), un módulo de comunicación (76) y un módulo de control (77).

El reglamento (78) contiene las restricciones negociadas contractualmente (p. ej. acuerdos sobre el nivel de servicio) en forma de especificaciones técnicas. Una especificación técnica puede definirse, en este sentido, de forma distinta, p. ej. mediante cláusulas o mediante variables de configuración cuyos atributos definen derechos de acceso dedicados a los recursos (6, 7, 8).

El módulo de comunicación (76) gestiona las interfaces (16) entre el entorno básico (5) y los entornos de usuario (3, 4) o las interfaces (11) entre el entorno básico (5) y los recursos (6, 7, 8), respectivamente. El canal de comunicación se protege a través del módulo de seguridad (79) contra un acceso no autorizado. Para ello, el módulo de seguridad (79) asiste a los mecanismos de identificación, autentificación y autorización así como a las tecnologías de codificación. El módulo de seguridad (79) contiene otras funciones básicas de seguridad para que el entorno básico (5), entre otras cosas, sea capaz de establecer, eliminar, asignar o resolver a partes (30, 31) y entornos de usuario (3, 4) y, dado el caso, verificar o utilizar para la autentificación o autorización las posibilidades de identificación (p.ej. certificados, códigos o similares). Las posibilidades de identificación pueden contener informaciones específicas de las partes, por ejemplo datos sobre los derechos de recursos (6, 7, 8) negociados para cada parte (30, 31). Así, las funciones de seguridad son una parte íntegra esencial del proceso de división de los derechos de acceso a los recursos (6, 7, 8) o participaciones de recursos (6, 7, 8) a las partes (30, 31) y la protección de los entornos de usuario (3, 4) y el entorno básico (5).

El módulo de control (77) sustituye, junto con el reglamento (78), al supervisor hasta ahora imprescindible para este tipo de sistemas.

El módulo de control (77) supervisa el cumplimiento de las especificaciones del reglamento (78). Determina el proceso de negociación mediante un procedimiento de proceso según el estado actual (figura 11). Según el resultado de las negociaciones, el módulo de control (77) adapta el reglamento (78). De esta manera, las restricciones no se definen por un supervisor, sino que se pueden negociar mediante un proceso técnico entre las partes (30, 31). Además, el módulo de control (77) implementa las modificaciones negociadas en la infraestructura. Genera, gestiona y elimina entornos de usuario (3, 4) y configura los recursos (6, 7, 8) que se usan de forma compartida, paralela por varias partes (30, 31). De esta forma, el módulo de control (77) sustituye al supervisor por completo mediante un componente técnico que se comporta de manera absolutamente neutral con lo que respecta a las partes (30, 31) de la infraestructura de uso compartido e implementa las restricciones negociadas en común con el reglamento (78). El propio módulo de control (77) no está sujeto a una administración superior mediante un supervisor. Su comportamiento, por el contrario, se predetermina por todas las partes (30, 31) del CAP de forma común y con los mismos derechos.

En resumen, el entorno básico (5) contiene funciones básicas firmes e interfaces (11, 16) para el acceso a los recursos (6, 7, 8) del CAP. Las funciones básicas en los módulos (por lo menos en el módulo de seguridad (78), módulo de control (77), módulo de comunicación (76), reglamento (78)) pueden ser encapsuladas y pueden realizar por lo menos lo siguiente:

- funciones que sustituyen a un supervisor hasta ahora imprescindible permitiendo, con ello, una administración y un uso con los mismos derechos y en común de la infraestructura, entre otros:

    1. Curso del proceso controlado por el estado (figura 11) como unidad técnica para la realización de un proceso neutral de negociación para la división con los mismos derechos y en común de los recursos (6, 7, 8) entre varias partes (30, 31) que administran o usan, respectivamente, de forma paralela la misma infraestructura.

    2. Un reglamento adaptativo (78) en forma de especificación técnica mediante, p. ej. cláusulas o variables de configuración para la realización de acuerdos sobre el nivel de servicio negociados.

    3. Lógica de proceso para la generación, administración y eliminación de los entornos de usuario (3, 4), según las especificaciones del reglamento (78).

    4. Lógica de monitorización para la monitorización del cumplimiento de las especificaciones del reglamento (78), en particular, monitorización del acceso a los recursos (6, 7, 8) del CAP.

- funciones de seguridad (p.ej. funciones de identificación, autentificación, autorización, monitorización de la integridad, codificación, detección de errores, respuesta a errores, entre otras)

- contabilidad

- funciones de sistema operativo tradicionales como, por ejemplo:

    1. Funciones de administración de sistemas de archivos.

    2. Funciones QoS (p.ej. monitorización de los tiempos de latencia del tráfico de datos).

3. Funciones de optimización (p.ej. funciones de distribución de carga).

4. Servicios de red (servidor o client DHCP, HTTP, FTP, TFTP).

5. Funciones de sistema (p.ej. puesta a disposición de interfaces (controladores) para acceder a los recursos de hardware del CAP).

El entorno básico (5) no puede alterarse, eliminarse, intercambiarse o ampliarse en sus funciones por las partes (30, 31) después del suministro del CAP por parte del fabricante. De esta forma, se asegura la neutralidad del entorno básico (5) (en particular del módulo de control (77) relacionado con el reglamento (78)). El acceso directo a las funciones básicas del entorno básico (5) no es posible, sino limitado mediante interfaces definidas (13, 15, 16) que existen entre el entorno básico (5) y el entorno/los entornos de usuario (figura 10) y se determinan a través del módulo de comunicación (76), el módulo de control (77) y el reglamento (78). En un principio, sólo se puede acceder a estas funciones básicas a través de los entornos de usuario (3, 4). No existen interfaces del entorno básico (5) directamente con los puntos de comunicación exteriores del CAP o de puntos de comunicación exteriores del CAP con el entorno básico (5), respectivamente. De esta forma, se impide que se pueda influir en el entorno básico (5) de cualquier forma mediante factores perturbadores externos o comprometerse de algún modo a causa de un ataque externo.

Las funciones básicas, por lo general, se dividen en funciones básicas configurables y funciones básicas fijas. Las funciones básicas configurables pueden ajustarse mediante modificaciones específicas de parámetros de función a través de interfaces definidas. Las funciones básicas fijas no comprenden parámetros variables. Un entorno básico (5) puede contener funciones básicas configurables y fijas o una combinación de configuraciones básicas configurables o fijas. Las configuraciones básicas pueden realizarse con técnica de software, con técnica de hardware o con una combinación de software y hardware.

Las diferentes informaciones sobre el uso de los recursos pueden protocolarse para cada parte (30, 31) mediante el entorno básico (5) (contabilidad). Según los derechos definidos en el reglamento (78), las partes (30, 31) pueden establecer protocolos sobre las informaciones recogidas, sin embargo, no pueden alterar los protocolos. Los protocolos pueden utilizarse para asistir a posibles mecanismos de facturación o para hacer transparente la facturación del uso de los recursos (6, 7, 8) para todas las partes (30, 31).

Un entorno de usuario (3, 4) limita los derechos de uso de los recursos (6, 7, 8) negociados contractualmente del CAP y los datos, así como las unidades de datos y funciones de una parte (30, 31) de otros entornos de usuario (3, 4). Para cada parte (30, 31) se establece un entorno de usuario (3, 4) en el CAP (figura 9). Los entornos de usuario (3, 4) están completamente desacoplados entre sí. No existen interfaces entre los entornos de usuario individuales (3, 4). De esta forma se impide, que una parte (30, 31) pueda penetrar a los entornos de usuario (3, 4) de otras partes o usar los derechos de uso de recursos (6, 7, 8) o de participaciones de recursos de entornos de usuario (3, 4) de las otras partes (30, 31). El acceso a los entornos de usuario (3, 4) se especifica precisamente mediante el reglamento (78) del entorno básico (5) y se asegura y supervisa mediante las funciones de seguridad del entorno de usuario (3, 4). De esta manera, sólo una parte (30, 31), que ha sido verificada por las funciones de seguridad, puede acceder a un entorno de usuario (3, 4). A una parte (30, 31) se le garantiza, a través del módulo de control (77) y el reglamento (78), el uso exclusivo de los recursos (6, 7, 8) especificados por los derechos de uso, y, a través del módulo de seguridad se aseguran los datos y unidades de datos de cada entorno de usuario (3, 4). Para cada parte (30, 31) su entorno de usuario (3, 4) parece tener un uso completamente individual. La parte (30, 31) posee la totalidad de los derechos de administración para su entorno de usuario (3, 4).

Por ejemplo, puede instalar el software o cualquier servicio y llevar a cabo configuraciones. La libertad de diseño del entorno de usuario (3, 4) sólo está sujeta a las restricciones definidas para esta parte (30, 31) por el reglamento (78) del entorno básico (5) y se supervisa mediante el módulo de control (77) del entorno básico (5). Esta libertad de diseño del entorno de usuario (3, 4) es una ventaja económica en comparación con los sistemas actualmente conocidos. Por ejemplo, los proveedores de servicios pueden trasladar servicios de su red principal a los puntos de acceso y, de esta manera, son mucho más flexibles en la puesta a disposición de los servicios y la configuración de sus redes. Los entornos de usuario (3, 4) de un CAP pueden usarse, por ejemplo, para la puesta a disposición de diferentes redes de acceso y como puntos de accesos a redes de diferentes proveedores de servicio. Cada parte (30, 31) puede adaptar, gracias a esta libertad de diseño de su entorno de usuario (3, 4), los mecanismos de seguridad de la red de acceso a sus propios mecanismos de seguridad. Así, la parte (30, 31) es completamente independiente de los mecanismos de seguridad de las otras partes (30, 31) en sus redes de acceso disponibles a través del mismo CAP. El tráfico de red de las diferentes redes de acceso puestas a disposición por el entorno de usuario (3, 4) no está conectado pero sí asegurado contra un acceso no autorizado (espías o falsificación de informaciones).

Los entornos de usuario (3, 4) de las otras partes (30, 31) no son visibles para la otra parte correspondiente (30, 31). Los recursos (6, 7) disponibles para cada parte (30, 31) pueden estimarse mediante los derechos de uso precisamente definidos de los recursos (6, 7) o participaciones de recursos (6, 7) y la garantía del uso exclusivo de estos recursos (6, 7) o participaciones de recursos (6, 7) de forma precisa. La parte (30, 31) puede planificar el uso de dichos recursos (6, 7).

La estimación precisa y la planificación de recursos (6, 7, 8) a pesar de un uso común de un CAP por varias partes (30, 31) suponen otra ventaja económicamente significativa en comparación con los sistemas conocidos actualmente. Por ejemplo, para los proveedores de servicios la planificación de recursos (6, 7, 8) es muy importante para hacer un cálculo sobre su oferta de servicios. Los proveedores de servicio, por consiguiente, son capaces de poder garantizar a sus clientes las ofertas de servicio.

Un entorno de usuario (3, 4) contiene por lo menos un módulo de comunicación (74, 75, 81), un módulo de seguridad (73, 80, 83) y un módulo de gestión (72, 82).

El módulo de gestión (72, 82) gestiona las interacciones entre el entorno de usuario (3, 4) y el entorno básico (5), así como entre el entorno de usuario (3, 4) y la correspondiente parte (30, 31). Mediante el módulo de gestión (72, 82), por ejemplo, pueden dirigirse e implementarse las solicitudes de modificación en los ajustes del entorno de usuario (3, 4) por la parte (30, 31). Así, el módulo de gestión (72, 82) interactúa con el módulo de control (77) del entorno básico (5) si los derechos de uso encapsulados en el entorno de usuario (3, 4) no fueran suficientes para la realización de las solicitudes de modificación y si se requiriesen, si fuera necesario, procesos de negociación con las otras partes (30, 31) del CAP antes de poder implementar las solicitudes de modificación. Por el otro lado, el módulo de gestión (72, 82) informa a la parte (30, 31) si existen solicitudes de modificación de las otras partes (30, 31) del CAP que requieran el consentimiento de la parte (30, 31).

El módulo de gestión (72) puede encontrarse en el entorno de usuario (3, 4) o el módulo de gestión (82) puede encontrarse fuera del CAP y estar integrado en un sistema autónomo de gestión (84). Si el módulo de gestión (82) se encuentra fuera del CAP, integrado en un sistema de gestión (84), el sistema de gestión (84) también comprenderá un módulo de comunicación (81) y un módulo de seguridad (80).

El módulo de comunicación (74, 75, 81) forma las interfaces entre el entorno de usuario (3, 4) y el entorno básico (5), y entre el entorno de usuario (3, 4) y su parte (30, 31) o el módulo de gestión (82) en su sistema externo de gestión (84) de la parte (30, 31).

El canal de comunicación se protege a través del módulo de seguridad (73, 80, 83) contra un acceso no autorizado. Para ello, el módulo de seguridad (73, 80, 83) asiste a los mecanismos de identificación, autentificación y autorización así como a las tecnologías de codificación. Las posibilidades de identificación pueden contener informaciones específicas sobre las partes, por ejemplo, datos sobre los derechos de uso de recursos (6, 7, 8) negociados para una determinada parte (30, 31). Así, las funciones de seguridad forman un componente íntegro esencial del proceso para la división de los derechos de acceso a los recursos (6, 7, 8) o las participaciones de recursos de las partes (30, 31) y la protección de los entornos de usuario (3, 4) y del entorno básico (5).

Para el acceso al entorno básico (5) y el o los entornos de usuario (3, 4) de un CAP o para el acceso a los recursos (6, 7, 8) de un CAP, respectivamente, se requieren varias interfaces (figura 10). Las interfaces se definen mediante los módulos de comunicación (74, 75, 81) de los entornos de usuario (3, 4) o mediante el módulo de comunicación (76) del entorno básico (5), respectivamente. Las interacciones a través de estas interfaces se aseguran mediante las funciones de los módulos de seguridad (73, 79, 80, 83) de los entornos de usuario (3, 4) y del entorno básico (5). La figura 10 muestra las interfaces necesarias con el ejemplo de dos partes (30, 31) (A y B) de un CAP. Esta ilustración no limita el uso también de una parte o más de dos de un CAP.

- Las interfaces I_{NA} (12) y I_{NB} (14) facilitan las interacciones entre las partes (30, 31) (A y B) con sus respectivos entornos de usuario (3, 4) de un CAP. Solo las partes (30, 31) que se han verificado con respecto a la seguridad técnica pueden acceder al entorno de usuario (3, 4) correspondiente.

- Las interfaces I_{NAB} (13) y I_{NBB} (15) sirven para la interacción entre los entornos de usuario (3, 4) (A y B) y el entorno básico (5). Esta interacción, entre otras cosas, es necesaria para que el entorno básico (5) pueda generar, alterar o eliminar entornos de usuario (3, 4) para las nuevas partes (30, 31). Además, estas interfaces (13, 15) se requieren para que los entornos de usuario (3, 4) puedan acceder a funciones básicas dedicadas del entorno básico (5).

- La interfaz I_{BN} (16) facilita el acceso a funciones básicas del entorno básico (5), sin embargo, sólo partiendo de la base de un entorno de usuario (3, 4) de este CAP. El entorno básico (5) no se puede acceder directamente desde los entornos (por ejemplo, desde un sistema de gestión (84) externo), fuera del CAP, sino sólo de forma indirecta a través de las interfaces (12, 14) de los entornos de usuario (3, 4) y a través de las interfaces (13, 15, 16) de los entornos de usuario (3, 4) para el entorno básico (5). El módulo de control (77) y el reglamento (78) del CAP definen a qué funciones básicas del entorno básico (5) de un entorno de usuario (3, 4) se puede acceder.

- Las interfaces I_{NAR} (9) y I_{NBR} (10) ponen a disposición las posibilidades de interacción entre los entornos de usuario (3, 4) y los recursos (6, 7) especificados para cada entorno de usuario (3, 4) por los derechos de uso o participaciones de recursos (6, 7). Estas interacciones pueden ser órdenes a la función, por ejemplo, del entorno de usuario (3, 4) que facilitan el uso de recursos (6, 7) de este entorno.

- La interfaz I_{BR} (11) facilita la interacción del entorno básico (5) con los recursos (6, 7, 8) del CAP. Mediante esta interfaz (11) se realiza, por ejemplo, la configuración y la monotorización de recursos (6, 7, 8) de un CAP mediante el entorno básico (5). Por ejemplo, esta interfaz (11) realiza la monotorización del cumplimiento de las restricciones que se especifican en el reglamento (78) para las partes (30, 31) del CAP.

- Las interfaces I_{RRA} (17) y I_{RRB} (18) son semipermeables. Es decir, es posible una interacción a partir del entorno básico (5) con los recursos específicos del usuario (6, 7). Por ejemplo, mediante el acceso a las funciones básicas dedicadas del entorno básico (5), se pueden implementar técnicamente por medio de las interfaces I_{BR} (11), I_{RRA} (17) y I_{RRB} (18) las restricciones del reglamento (78) para la asignación de derechos de uso de recursos (6, 7, 8) o participaciones de recursos (6, 7, 8) a los entornos de usuario (3, 4). Sin embargo, una interacción a partir de los recursos (6, 7) delimitados por los derechos de uso de un entorno de usuario (3, 4) con unos recursos (6, 7, 8) para los que no existen derechos de uso, no es practicable según la definición del procedimiento basado en Cuckoo y será impedida por el módulo de control (77) del entorno básico (5).

La definición de interfaces determina las opciones de acceso, pero no el modo de acceso a los entornos (3, 4, 5) o recursos (6, 7, 8). Por ejemplo, el modo de acceso puede especificarse mediante cualquier protocolo, por ejemplo, SSH, HTTP, Telnet, FTP, TFTP, DHCP, SOAP, SNMP, TR069 mediante accesos de funciones locales o remotas, por ejemplo, COBRA, RMI, RPC, servicios web por medio de unos principios basados en agente, por ejemplo, agentes móviles, u otros métodos.

Para la negociación de los derechos de uso para recursos los (6, 7, 8) del CAP se requieren unos procesos representados a modo de ejemplo en la figura 12 con dos partes (30, 31) (A y B) de un CAP. Esta ilustración no limita el uso de también una parte o más de dos partes conjuntamente de un CAP.

La negociación de los derechos de uso entre las partes (30, 31) puede realizarse de forma controlada con respecto al estado. Por ejemplo, para el CAP se definen los tres estados idle (26), prepared (27) y ready (28) (figura 11).

Después de la entrega por parte del fabricante, el CAP puede encontrarse en uno de los dos estados básicos (19) idle (26) o ready (28).

En (20) el estado idle (28), el CAP contiene el entorno básico (5) y un entorno de usuario (3) para la parte A (30). A la parte A (30) ya se le ha emitido, a través del módulo de seguridad (79) del entorno básico (5), una opción de identificación válida para el acceso a su entorno de usuario (3). Esta opción de identificación se le notifica, por ejemplo, por escrito, a la parte A (30) con la entrega del CAP por parte del fabricante. En este caso, la parte A (30) es la propietaria del CAP. Los derechos de uso de los recursos (6) del CAP están completamente asignados a la parte A (30) o están contenidos completamente en su entorno de usuario (3). El reglamento (78) del entorno básico (5) está configurado correspondientemente. Con el primer acceso exitoso al entorno de usuario (3) por la parte A (30) (después de una identificación satisfactoria), el CAP cambia (21) al estado ready (28).

Se alcanza el estado prepared (27), siempre y cuando

1. deba(n) crearse uno o varios entornos de usuario nuevos (3, 4),

2. las restricciones de los entornos de usuario (3, 4) deban ser modificadas (por ejemplo, modificaciones de los derechos de uso), o los ajustes del CAP que vayan más allá de los derechos de uso de los entornos de usuario (3, 4) deban ser modificados, o

3. deba(n) borrarse uno o varios entornos de usuario nuevos (3, 4).

Para ello, o bien se transmite al CAP una solicitud de modificación por una parte (30, 31) del CAP, o bien unas restricciones de entornos de usuario (3, 4) han vencido o han sido violadas por las partes (30, 31).

El caso (1) se da cuando una parte (30, 31) (por ejemplo, la parte A (30)) cede parcial o completamente los derechos de uso de los recursos (6, 7) de un CAP otorgados a la misma a un tercero (por ejemplo, a la parte B (31)). Con ello, se realizan los siguientes procesos:

La parte A (30) elige una participación correspondiente de sus recursos (6) del CAP para una cesión a, en este ejemplo, una parte potencial B (31). La selección de los recursos (6, 7) representa una interacción de la parte (30, 31) con su entorno de usuario (3, 4). Por consiguiente, dicha selección se efectúa mediante la interfaz I_{NA} (12).

Para ello, una consulta por la parte A (30) para determinar informaciones sobre los recursos propios disponibles (6) de la parte A (30) se transmite primero al módulo de comunicación (74) y después mediante el módulo de seguridad (73) al módulo de gestión (72). De esta manera, la ruta de transmisión para esta interacción sería, con respecto a los números de referencia en la figura 12, la siguiente: 32->33->34. Sin restringir la validez general, se supone que el módulo de gestión (72) está dispuesto dentro del entorno de usuario A (3). El módulo de seguridad (73) verifica la opción de identificación de la parte A (30). Solamente después de una autenticación satisfactoria la consulta pasará al módulo de gestión (72). El módulo de gestión (72) determina las informaciones sobre los recursos disponibles (6) al transmitir, mediante el módulo de seguridad (73) y mediante el módulo de comunicación (74) del entorno de usuario A (3), una consulta mediante las interfaces (13, 16), mediante el módulo de comunicación (76) y mediante el módulo de seguridad (79) al módulo de control (77) del entorno básico (5). La ruta de transmisión para esta interacción sería, con respecto a los números de referencia en la figura 12, la siguiente: 35->36->37->38->39. El módulo de

seguridad (79) verifica la opción de identificación de la parte A (30) o del entorno de usuario A (3). Solamente después de una autenticación satisfactoria la consulta pasará (39) al módulo de control (77). El módulo de control (77) determina a partir del reglamento (78) las informaciones solicitadas y transmite las informaciones mediante el módulo de seguridad (79), el módulo de comunicación (76) del entorno básico (5), las interfaces (16, 13), el módulo de comunicación (74), y el módulo de seguridad (73) al módulo de gestión (72) del entorno de usuario A (3). Es decir, la ruta de transmisión para esta interacción sería, con respecto a los números de referencia en la figura 12, la siguiente: 40->57->58->59->60. El módulo de gestión (72) facilita las informaciones a la parte A (30) mediante el módulo de seguridad (73), el módulo de comunicación (74) y la interfaz I_{NA} (12). Es decir, la ruta de transmisión para esta interacción sería, con respecto a los números de referencia en la figura 12, la siguiente: 61->62->63. A partir de las informaciones sobre los recursos seleccionados, junto con un período de cesión establecido por la parte A (30), y sobre la parte A (30) seleccionada a la que haya que ofertar los recursos (por ejemplo, la parte B (31)), se genera una solicitud de modificación por el módulo de gestión (72) del entorno de usuario A (3). Esta solicitud de modificación puede ser especificada con distintos lenguajes que se pueden evaluar mecánicamente (por ejemplo, XML). La solicitud de modificación se transmite al módulo de control (77) del entorno básico (5) mediante el módulo de seguridad (73), el módulo de comunicación (74) del entorno de usuario A (3), la interfaz I_{NAB} (13) y la interfaz I_{BN} (16), mediante el módulo de comunicación (76) y el módulo de seguridad (79). Es decir, la ruta de transmisión para esta interacción sería, con respecto a los números de referencia en la figura 12, la siguiente: 35->36->37->38->39.

Durante la entrega, el módulo de seguridad (79) del entorno básico (5) verifica primero la identidad de la parte A (30) o del entorno de usuario A (3). Solamente si la identidad ha sido confirmada con éxito mediante la opción de identificación del usuario A, se aceptará la recepción de la solicitud de modificación por el entorno básico (5) o se transmitirá la misma del módulo de seguridad (79) al módulo de control (77). En su defecto, la identidad del usuario A también puede ser aceptada como válida mediante una opción de identificación verificada con éxito del entorno de usuario A (3) frente al entorno básico (5), si la parte A (30) se ha identificado previamente ella misma con éxito frente al entorno de usuario A (3). El módulo de control (77) verifica las informaciones contenidas en la solicitud de modificación con la ayuda del reglamento (78). Así, por ejemplo, no es posible que la selección de recursos deseada en la solicitud de modificación contenga participaciones para las que el solicitante de la solicitud de modificación -en este caso, la parte A (30)- no posea ninguna autorización de acceso, por ejemplo, para recursos según (7, 8). Después de la verificación exitosa de la opción de identificación mediante el módulo de seguridad (79) y la validez de la solicitud de modificación mediante el módulo de control (77) del entorno básico (5), el CAP cambia al estado “prepared 27”.

Mediante el módulo de seguridad (79) del entorno básico (5) se genera, en caso necesario, una nueva opción de identificación para la parte A (30) y una nueva opción de identificación para la parte potencial B (31). Esta opción de identificación puede contener informaciones específicas del usuario o puede estar ligada de alguna manera con informaciones específicas de usuario. Por ejemplo, las informaciones específicas de usuario describen los derechos de uso de los recursos que la nueva parte B (31) pueda solicitar como máximo, y el valor para la duración de uso máxima para los derechos de uso de los recursos solicitados. Dichos derechos de uso que se pueden seleccionar como máximo y dicha duración de uso que se puede seleccionar como máximo corresponden a las informaciones que la parte A (30) haya definido para la cesión en la solicitud de modificación. El módulo de control (77) del entorno básico (5) genera, a partir de la solicitud de modificación, una oferta de recursos para la parte potencial B (31) que contiene por lo menos las informaciones según la solicitud de modificación de la parte A (30), es decir, la selección de recursos y el período para la cesión. Además, se pueden integrar informaciones adicionales en esta oferta de recursos mediante el entorno básico (5), por ejemplo, una opción de identificación para la parte B (31). La oferta de recursos es una especificación técnica que puede ser definida en varios lenguajes de especificación, por ejemplo, XML, o con la ayuda de unas variables de configuración. El entorno básico (5) transmite la oferta de recursos a la parte potencial B (31). En esta forma de realización, la parte B (31) posee un sistema de gestión (84) externo al CAP, sin restringir la validez general. Debido a la restricción con respecto a la seguridad técnica consistente en el hecho de que el entorno básico (5) no posea ninguna opción de comunicación directa con los puntos de comunicación fuera del CAP, la oferta de recursos se transmite de forma indirecta, mediante el entorno de usuario A (3) -es decir, mediante el módulo de seguridad (79, el módulo de comunicación (76) del entorno básico (5), mediante las interfaces, empezando por I_{BN} (16) y después I_{NAB} (13), y de allí mediante el módulo de comunicación (74), verificado por el módulo de seguridad (73) del entorno de usuario A (3) del sistema de gestión, y de allí mediante el módulo de comunicación (80) y el módulo de seguridad (81)- al módulo de gestión (82) de la parte B (31). La transmisión indirecta está asegurada adicionalmente por el módulo de seguridad (79) del entorno básico (5), de modo que durante el proceso de comunicación se puedan detectar modificaciones en cuanto al contenido de la oferta de recursos y que el contenido de la oferta de recursos solamente sea detectable por el módulo de control (77) del entorno básico (5) y por el módulo de gestión (82) de la parte potencial B (31). Si se detectan modificaciones en la oferta de recursos, la oferta de recursos será invalidada inmediatamente.

Es decir, la ruta de transmisión para esta interacción sería, con respecto a los números de referencia en la figura 12, la siguiente: 56->57->85->67->68.

La oferta sobre recursos es recibida por el módulo de gestión (82) de la parte potencial B (31). El módulo de gestión le presenta la oferta de recursos a la parte B (31) mediante el módulo de seguridad (81), el módulo de comunicación (80) y la interfaz (29) del sistema de gestión (84). Es decir, la ruta de transmisión para esta interacción sería, con respecto a los números de referencia en la figura 12, la siguiente: 69->70->71.

La parte potencial B (31) puede elegir para qué recursos de la oferta de recursos desea adquirir los derechos de uso y para qué período. Los derechos de uso y la duración de uso pueden ser elegidos según el máximo establecido

en la oferta de recursos. Si la parte B (31) ha decidido aceptar o rechazar la oferta, se transmite una información correspondiente de la parte B (31) mediante la interfaz (29) del sistema de gestión (84), el módulo de comunicación (80), el módulo de seguridad (81) al módulo de gestión (82) del sistema de gestión (84). El módulo de seguridad (81) verifica la opción de identificación de la parte B (31). La información se transmite al módulo de gestión (82) solamente después de una verificación exitosa de la opción de identificación.

De vez en cuando, el módulo de control (77) del entorno básico (5) le consulta al módulo de gestión (82) de la parte B (31) el estado de la oferta de recursos indirectamente por medio del entorno de usuario A (3), es decir, por medio del módulo de seguridad (79), el módulo de comunicación (76) del entorno básico (5), mediante las interfaces empezando por I_{BN} (16) y después I_{NAB} (13), y de allí mediante el módulo de comunicación (74) del entorno de usuario A (3) mediante la interfaz I_{NA} (12) a la interfaz (29) del sistema de gestión, y de allí mediante el módulo de comunicación (80) y el módulo de seguridad (81). De esta manera, la transmisión indirecta es asegurada adicionalmente mediante el módulo de seguridad (79) del entorno básico (5), de modo que la consulta sea detectable solamente para el módulo de control (77) del entorno básico (5) y el módulo de gestión (82) de la parte potencial B (31).

Es decir, la ruta de transmisión para esta interacción sería, con respecto a los números de referencia en la figura 12, la siguiente: 56->57->85->67->68.

La respuesta a la consulta de estado se transmite mediante la ruta de transmisión, que sería, con respecto a los números de referencia en la figura 12: (69->70->85->38->39), del módulo de gestión (82) del sistema de gestión (84) indirectamente mediante el entorno de usuario A (3) al módulo de control (77) del entorno básico (5). De esta manera, la transmisión indirecta es asegurada adicionalmente mediante el módulo de seguridad (81) del sistema de gestión (84), de modo que la consulta sea detectable solamente para el módulo de control (77) del entorno básico (5) y el módulo de gestión (82) de la parte potencial B (31). El módulo de seguridad (79) verifica la opción de identificación del sistema de gestión (84). Solamente después de una autenticación satisfactoria la respuesta será transmitida al módulo de control (77).

Si la parte B (31) se ha decidido a favor de la oferta de recursos, la respuesta contiene informaciones sobre las participaciones de recursos y la duración de uso que la parte B (31) haya elegido de la oferta de recursos. En este caso, se efectúa el siguiente proceso técnico mediante el entorno básico (5):

El entorno básico (5) genera para la nueva parte B (31) un nuevo entorno de usuario B (4) en el CAP sujeto a las restricciones de los derechos de uso elegidos y la duración de uso elegida de la respuesta recibida para la oferta de recursos. Al mismo tiempo, se ajusta el entorno de usuario A (3) de la parte A (30) correspondientemente. Es decir, a la parte A (30) se le retiran los derechos de uso o al entorno de usuario A (3) se le retiran los recursos para los recursos cedidos a la parte B (31). La retirada de los derechos de uso de recursos para la parte A (30) o la retirada de recursos para el entorno de usuario A (3) así como el otorgamiento de nuevos derechos de uso de recursos cedidos para la parte B (31) o la entrega de recursos (7) al entorno de usuario B (4) se efectúan mediante el módulo de control (77) del entorno básico (5), adaptándose las especificaciones del reglamento (78) de forma correspondiente. El módulo de control (77) del entorno básico (5) le señala a la parte A (30) y a la parte B (31) que la solicitud de modificación se ha realizado.

La información sobre la realización de la solicitud de modificación se transmite por el módulo de control (77) del entorno básico (5) al módulo de gestión (72) del entorno de usuario A (3) mediante la ruta de transmisión 56->57>58->59->60, según los números de referencia de la figura 12. El módulo de seguridad (73) verifica la opción de identificación del entorno básico (5). La información se transmite al módulo de gestión (72) solamente después de una verificación exitosa de la opción de identificación.

Además, la información sobre la realización de la solicitud de modificación se transmite por el módulo de control (77) del entorno básico (5) al módulo de gestión (82) del sistema de gestión (84) mediante la ruta de transmisión 40->41->42->43->44->45->46->47, según los números de referencia de la figura 12. El módulo de seguridad (81) verifica la opción de identificación del entorno básico (5). La información se transmite al módulo de gestión (82) solamente después de una verificación exitosa de la opción de identificación.

Ahora, el CAP está configurado solamente para dos partes (30, 31). El CAP cambia (22) al estado ready (28).

En el caso de que la respuesta a la consulta de estado de la oferta de recursos del entorno básico (5) señale que la oferta de recursos haya sido rechazada por la parte B (31), el entorno básico (5) efectúa los siguientes procesos técnicos:

La oferta de recursos es retirada y borrada por el módulo de control (77) del entorno básico (5). El módulo de control (77) reinicializa el CAP para volver a su configuración inicial en la que se había encontrado el CAP antes de la solicitud de modificación recibida. Esto significa que las opciones de identificación posiblemente generadas para la parte potencial B (31) sean borradas. Además, el módulo de control (77) del entorno básico (5) le señala al módulo de gestión (72) de la parte A (30), mediante las interfaces, empezando por I_{BN} (16) y después I_{NAB} (13) y de allí mediante el módulo de comunicación (74) y el módulo de seguridad (73) que la solicitud de modificación ha sido rechazada y que no será implementada por el módulo de control (77) del entorno básico (5). El módulo de seguridad (73) verifica la opción de identificación del entorno básico (5). La información se transmite al módulo de gestión (72) solamente después de una verificación exitosa de la opción de identificación.

Es decir, la ruta de transmisión para esta interacción sería, con respecto a los números de referencia en la figura 12, la siguiente: 56->57->58->59->60. La parte A (30) es informada de forma correspondiente por el módulo de gestión (72).

El CAP sigue estando configurado solamente para la parte A (30). Todos los derechos de uso concedidos antes de la solicitud de modificación a la parte A (30) permanecen con la parte A (30), o todos los recursos (6) encapsulados antes de la solicitud de modificación en el entorno de usuario A (3) permanecen en el entorno de usuario A (3). La especificación del reglamento (78) del entorno básico (5) no es modificada por el módulo de control (77) del entorno básico 5) sino que mantiene exactamente la misma configuración que antes de la solicitud de modificación. El CAP cambia (22) al estado ready (28).

En el caso (2), sin restringir la validez general, una parte (30, 31), a continuación la parte A (30), de un CAP desea modificaciones en los ajustes de su entorno de usuario sin restringir la validez general, a continuación el entorno de usuario A (30). La selección de los ajustes a modificar representa una interacción de la parte A (30) con su módulo de gestión (72) del entorno de usuario A (3). Por consiguiente, dicha selección se realiza mediante la interfaz I_{NA} (12), el módulo de comunicación (74) y el módulo de seguridad (73) al módulo de gestión (72) del entorno de usuario A (3).

El módulo de seguridad (73) verifica la opción de identificación de la parte A (30). La información se transmite al módulo de gestión (72) solamente después de una verificación exitosa de la opción de identificación.

Es decir, la ruta de transmisión para esta interacción sería, con respecto a los números de referencia en la figura 12, la siguiente: 32->33->34.

Las modificaciones pueden influir directamente en los ajustes de otros entornos de usuario de un CAP. Si las modificaciones influyen en otros entornos de usuario o no, se puede detectar por los derechos de uso de la parte. Las modificaciones que no se pueden implementar solamente con los derechos de uso de una parte, sino que también afectan a los recursos que no están dentro del ámbito de los derechos de uso de la parte, es decir, cuando existen, por ejemplo, derechos de uso de estos recursos por otras partes, requieren el consentimiento de estas partes antes de implementar las modificaciones. Por este motivo, se genera una solicitud de modificación a partir de las informaciones sobre las modificaciones seleccionadas por el módulo de gestión (72) de la parte A (30). Esta solicitud de modificación puede ser especificada con distintos lenguajes que se pueden evaluar mecánicamente (por ejemplo, XML). La solicitud de modificación se transmite al módulo de control (77) del entorno básico (5) mediante el módulo de seguridad (73) y el módulo de comunicación (74) del entorno de usuario A (3), mediante la interfaz I_{NAB} (13) y la interfaz I_{BN} (16), mediante el módulo de comunicación (76) y el módulo de seguridad (79).

El módulo de seguridad (79) verifica la opción de identificación de la parte A (3). La información se transmite al módulo de control (77) solamente después de una verificación exitosa de la opción de identificación.

Es decir, la ruta de transmisión para esta interacción sería, con respecto a los números de referencia en la figura 12, la siguiente: 35->36->37->38->39.

El módulo de control (77) neutral con respecto a las partes verifica las informaciones contenidas en la solicitud de modificación con la ayuda del reglamento (78).

Para ello, el CAP cambia (24) al estado “prepared (27)”.

Mediante las informaciones del reglamento (78), el módulo de control (77) sabe cuál es la influencia de la implementación de las modificaciones en los ajustes definidas en la solicitud de modificación sobre los entornos de usuario ya existentes (3, 4).

El módulo de control (77) transmite una consulta de modificación a todas las partes (30, 31) del CAP cuyo entorno de usuario es influenciado por los deseos de ajuste contenidos en la solicitud de modificación de la parte A (30). A continuación, sin restringir la validez general, se parte de la base de que el entorno de usuario B (4) sea influenciado por la implementación de los deseos de ajuste de la parte A (30).

En este caso, el módulo de control (77) del entorno básico (5) transmite una consulta de modificación al módulo de gestión (82) de la parte B (31) mediante el módulo de seguridad (79) y el módulo de comunicación (76) del entorno básico (5), mediante las interfaces I_{BN} (16), I_{NBB} (15) e I_{NB} (14) a la interfaz (29) y allí mediante el módulo de comunicación (80) y el módulo de seguridad (81) del sistema de gestión (84). Primero, el entorno básico (5) se identifica frente al módulo de seguridad (81) del sistema de gestión (84) de la parte B (31) con su opción de identificación. Solamente después de la identificación exitosa, el sistema de gestión de la parte B (31) acepta la recepción de la consulta de modificación. Además, la transmisión indirecta es asegurada adicionalmente mediante el módulo de seguridad (79) del entorno básico (5), de modo que la solicitud de modificación sea detectable solamente para el módulo de control (77) del entorno básico (5) y mediante el módulo de gestión (82) del sistema de gestión (84).

Es decir, la ruta de transmisión para esta interacción sería, con respecto a los números de referencia en la figura 12, la siguiente: 40->41->42->43->44->45->46->47.

El módulo de gestión (82) señala a la parte B (31) una nueva consulta de modificación mediante el módulo de seguridad (81), el módulo de comunicación (80) y la interfaz (29) del sistema de gestión (84).

Es decir, la ruta de transmisión para esta interacción sería, con respecto a los números de referencia en la figura 12, la siguiente: 69->70->71.

Ahora, la parte B (31) tiene la posibilidad de aceptar la consulta de modificación, o de rechazarla.

El módulo de control (77) del entorno básico (5) recibe la respuesta a la consulta de modificación o bien mediante la señalización por el módulo de gestión (82) de la parte B (31), después de que la parte B (31) haya tomado su decisión con respecto a la aceptación o la denegación, o bien mediante una consulta repetida en ciertos intervalos del estado de la consulta de modificación al módulo de gestión (82) de la parte B (31), hasta que la parte B (31) haya tomado su decisión sobre la aceptación o la denegación. Es decir, la ruta de transmisión para esta interacción sería, con respecto a los números de referencia en la figura 12, la siguiente: 48->49->50->51->52->53->54->55.

Cuando todas las partes a las que se haya transmitido una consulta de modificación como consecuencia de la solicitud de modificación de la parte A (30) hayan dado su consentimiento a la respectiva consulta de modificación -en este caso, por ejemplo, la parte B (31)- el módulo de control (77) del entorno básico (5) efectúa el siguiente proceso técnico:

Las modificaciones de los ajustes se implementan según la solicitud de modificación de la parte A (30) mediante el módulo de control (77) del entorno básico (5). En su caso, el reglamento (78) del entorno básico (5) se adapta correspondientemente. A todas las partes cuyo entorno de usuario esté afectado por estas modificaciones en los ajustes se les genera, en su caso, mediante el módulo de seguridad (79) del entorno básico (5), una nueva opción de identificación, respectivamente - en este ejemplo, a la parte A (30) y a la parte B (31). A todas las partes cuyo entorno de usuario sea afectado por estas modificaciones de los ajustes se les señala la implementación de las modificaciones de los ajustes - en este ejemplo, a la parte A (30) y a la parte B (31).

Para ello, se transmite una confirmación de la solicitud de modificación implementada y realizada por el módulo de control (77) del entorno básico (5) al módulo de gestión (72) de la parte A (30), mediante el módulo de seguridad (79) y el módulo de comunicación (77) del entorno básico (5), mediante las interfaces I_{BN} (16), I_{NAB} (13), el módulo de comunicación (74) y el módulo de seguridad (73) del entorno de usuario A (3). El módulo de seguridad (73) verifica la opción de identificación del entorno básico (5). La información se transmite al módulo de gestión (72) solamente después de una verificación exitosa de la opción de identificación.

Es decir, la ruta de transmisión para esta interacción sería, con respecto a los números de referencia en la figura 12, la siguiente: 56->57->58->59->60. En su caso, se le transmite a la parte A (30) una nueva opción de identificación generada mediante esta misma ruta de transmisión. La parte A (30) es informada por el módulo de gestión (72) del entorno de usuario A (3) -o bien mediante la señalización por parte del módulo de gestión (72) a la parte A (30), o bien mediante una consulta de la parte A (30) al módulo de gestión (72)- por lo menos sobre el módulo de seguridad (73), el módulo de comunicación (74) y la interfaz I_{NA} (12).

La ruta de transmisión para esta interacción sería, según los números de referencia en la figura 12, la siguiente: 61->62->63.

Además, se transmite una confirmación de la solicitud de modificación realizada e implementada del módulo de control (77) del entorno básico (5) al módulo de gestión de la parte B (31), mediante el módulo de seguridad (79) y el módulo de comunicación (76) del entorno básico (5), mediante las interfaces I_{BN} (16), I_{NBB} (15) e I_{NB} (14) a la interfaz (29) y allí mediante el módulo de comunicación (80) y el módulo de seguridad (81) del sistema de gestión (84). Primero, el entorno básico (5) se identifica ante el módulo de seguridad (81) del sistema de gestión (84) de la parte B (31) con su opción de identificación. Solamente después de la identificación satisfactoria el sistema de gestión de la parte B (31) aceptará la recepción de la información. Además, la transmisión es asegurada adicionalmente por el módulo de seguridad (79) del entorno básico (5), de modo que la información solamente sea detectable mediante el módulo de control (77) del entorno básico (5) y mediante el módulo de gestión (82) del sistema de gestión (84).

Es decir, la ruta de transmisión para esta interacción sería, con respecto a los números de referencia en la figura, 12 la siguiente: 56->64>65->43->44->66->67->68.

El módulo de gestión (82) señala a la parte B (31) una nueva consulta de modificación mediante el módulo de seguridad (81), el módulo de comunicación (80) y la interfaz (29) del sistema de gestión (84).

Es decir, la ruta de transmisión para esta interacción sería, con respecto a los números de referencia en la figura 12, la siguiente: 69->70->71. En su caso, se transmite una nueva opción de identificación generada a la parte B (31).

El CAP cambia (22) del estado “prepared (27)” al estado “ready (28)”.

Si una de las partes (30, 31) a las que se haya transmitido una consulta de modificación como consecuencia de la solicitud de modificación de la parte A (30) ha rechazado su respectiva consulta de modificación - en este caso, por ejemplo, la parte B (31), el módulo de control (77) del entorno básico (5) efectuará el siguiente proceso técnico:

La solicitud de modificación no se implementará por el módulo de control (77) del entorno básico (5). No se realizará modificación alguna en los ajustes. A todas las partes (30, 31) que hayan sido informadas sobre la solicitud de modificación con una consulta de modificación se les señala que no se ha efectuado ninguna implementación de la solicitud de modificación - es decir, en este caso a la parte A (30) y la parte B (31).

Para ello, se transmite una denegación de la solicitud de modificación consultada por el módulo de control (77) del entorno básico (5) al módulo de gestión (72) de la parte A (30), mediante el módulo de seguridad (79) y el módulo de comunicación (77) del entorno básico (5), mediante las interfaces I_{BN} (16), I_{NAB} (13), el módulo de comunicación (74) y el módulo de seguridad (73) del entorno de usuario A (3). El módulo de seguridad (73) verifica la opción de identificación del entorno básico (5). La denegación se transmite al módulo de gestión (72) solamente después de una verificación exitosa de la opción de identificación.

Es decir, la ruta de transmisión para esta interacción sería, con respecto a los números de referencia en la figura 12, la siguiente: 56->57->58->59->60.

Además, el módulo de control (77) del entorno básico (5) transmite una revocación de la consulta de modificación al módulo de gestión (82) de la parte B (31), mediante el módulo de seguridad (79) y el módulo de comunicación (76) del entorno básico (5), mediante las interfaces I_{BN} (16), I_{NBB} (15) y I_{NB} (14) a la interfaz (29) y allí mediante el módulo de comunicación (80) y el módulo de seguridad (81) del sistema de gestión (84). Primero, el entorno básico (5) se identifica ante el módulo de seguridad (81) del sistema de gestión (84) de la parte B (31) con su opción de identificación. Solamente después de la identificación satisfactoria, el sistema de gestión de la parte B (31) acepta la recepción de la revocación. Además, la transmisión es asegurada adicionalmente mediante el módulo de seguridad (79) del entorno básico (5), de modo que la revocación sea detectable solamente mediante el módulo de control (77) del entorno básico (5) y mediante el módulo de gestión (82) del sistema de gestión (84).

Es decir, la ruta de transmisión para esta interacción sería, con respecto a los números de referencia en la figura 12, la siguiente: 56->64->65->43->44->66->67->68.

El CAP cambia (22) del estado “prepared (27)” al estado “ready (28)”.

El borrado de un entorno de usuario puede producirse debido a una solicitud de modificación -según el caso (3)- por el vencimiento de una restricción acordada (por ejemplo, vencimiento de la duración de uso de los derechos de uso) o por un comportamiento no autorizado de la parte de un entorno de usuario.

El borrado de un entorno de usuario se inicia por medio del módulo de control (77) del entorno básico (5). A continuación, sin restringir la validez general, a la parte B (31) se le retira el entorno de usuario B (4). La opción de identificación de la parte B (31) se borra mediante el módulo de control (77) del entorno básico (5). Los recursos (7) encapsulados en el entorno de usuario B (4) se liberan mediante el módulo de control (77) del entorno básico (5). Ahora, los recursos (7) liberados o los derechos de uso retirados pueden ser entregados a otras partes (u otra parte). Por ejemplo, los derechos de uso pueden pasar de nuevo al propietario del CAP (en este caso la parte A (30)).

Para ello, el entorno de usuario A (3) de la parte A (30) se amplia en estos recursos (7) liberados, o sus derechos de uso se amplían en los derechos de uso de estos recursos (7). El módulo de control (77) implementa esta ampliación del entorno de usuario A (3) y adapta las especificaciones del reglamento (78) según estas modificaciones:

- borrado de las especificaciones para el entorno de usuario B (4)
- adaptación de las especificaciones para el entorno de usuario A (3).

En su caso, se genera para la parte A (30) una nueva opción de identificación mediante el módulo de seguridad (79) del entorno básico (5). Se transmite una información sobre la ampliación del entorno de usuario A (3) y, en su caso, una nueva opción de identificación al módulo de gestión (72) de la parte A (30), mediante el módulo de seguridad (79) y el módulo de comunicación (77) del entorno básico (5), mediante las interfaces I_{BN} (16), I_{NAB} (13), el módulo de comunicación (74) y el módulo de seguridad (73) del entorno de usuario A (3). El módulo de seguridad (73) verifica la opción de identificación del entorno básico (5). La información se transmite al módulo de gestión (72) solamente después de una verificación exitosa de la opción de identificación.

Es decir, la ruta de transmisión para esta interacción sería, con respecto a los números de referencia en la figura 12, la siguiente: 56->57->58->59->60. Las informaciones específicas del usuario posiblemente contenidas en la opción de identificación corresponden a las restricciones modificadas (nuevos derechos de uso). La parte A será notificada sobre la ampliación del módulo de gestión (72) del entorno de usuario A (3).

El módulo de gestión (82) del sistema de gestión (84) de la parte B (31) será informado sobre la retirada de sus derechos de uso y el borrado del entorno de usuario B por parte del módulo de control (77) del entorno básico (5). Para ello, el módulo de control (77) del entorno básico (5) transmite, antes del borrado del entorno de usuario B, una información correspondiente al módulo de gestión (82) de la parte B (31) mediante el módulo de seguridad (79) y el módulo de comunicación (76) del entorno básico (5), mediante las interfaces I_{BN} (16), I_{NBB} (15) y I_{NB} (14) a la interfaz (29) y allí mediante el módulo de comunicación (80) y el módulo de seguridad (81) del sistema de gestión (84). Primero, el entorno básico (5) se identifica ante el módulo de seguridad (881) del sistema de gestión (84) de la parte B (31) con su opción de identificación. Solamente después de la identificación satisfactoria, el sistema de gestión de la parte B (31) aceptará la recepción de la información. Además, la transmisión es asegurada adicionalmente por el módulo de seguridad (79) del entorno básico (5), de modo que la información solamente sea detectable mediante el módulo de control (77) del entorno básico (5) y mediante el módulo de gestión (82) del sistema de gestión (84). Es decir, la ruta de transmisión para esta interacción sería, con respecto a los números de referencia en la figura 12, la siguiente: 56->64->65->43->44->66->67->68. El CAP cambia (22) del estado "prepared (27)" al estado "ready (28)".

Para que el CAP pueda cambiar después de un tiempo finito al estado ready (28), pueden definirse unos tiempos de vencimiento finitos para el estado prepared (27). Es decir, aunque, por ejemplo, la solicitud de modificación aún no se haya implementado por el entorno básico (5), por ejemplo, porque no todas las partes hayan tomado una decisión con respecto a las consultas de modificación para la solicitud de modificación, la solicitud de modificación puede ser cancelada. Un tiempo de vencimiento determina por cuánto tiempo puede existir una solicitud de modificación sin ser confirmada. Después de exceder el tiempo de vencimiento, la solicitud de modificación será rechazada como no confirmada por el entorno básico (5) o será revocada. Las modificaciones no se implementarán por el entorno básico (5) y la especificación del reglamento (78) no será modificada. El módulo de control (77) del entorno básico (5) transmite a todos los módulos de gestión de las partes (30, 31) que hayan confirmado la solicitud de modificación dentro del tiempo de vencimiento, mediante la interfaz I_{BN} y las interfaces correspondientes de los entornos de usuario (3, 4) de estas partes (30, 31), una revocación confirmada mediante los módulos de seguridad del entorno básico (5) y los entornos de usuario correspondientes (3, 4), tal y como ya se ha descrito (véase el transcurso del proceso para el caso en el que una parte haya rechazado una consulta de modificación). El módulo de gestión de la parte que haya emitido la solicitud de modificación será informado por el módulo de control (77) del entorno básico (5) mediante el rechazo. El módulo de control (77) del entorno básico (5) transmite para ello al módulo de gestión de esta parte una denegación para la solicitud de modificación mediante la interfaz I_{BN} (16) y las interfaces correspondientes del entorno de usuario de esta parte (30, 31), confirmada mediante los módulos de seguridad del entorno básico (5) y de este entorno de usuario, tal y como ya se ha descrito (véase el transcurso del proceso para el caso en el que una parte haya denegado una consulta de modificación). El CAP cambia (22) al estado ready (28).

En un CAP que se encuentra en (23) el estado ready (28) todos los entornos de usuario (3, 4) del CAP están fijados establemente. En este caso, el término establemente se refiere a que todos los entornos de usuario (3, 4) del CAP están implementados completamente con unas restricciones válidas especificadas en el reglamento (78) del entorno básico (5). Todas las partes (30, 31) pueden acceder a su entorno de usuario (3, 4) correspondiente mediante su opción de identificación y pueden configurar el mismo libremente dentro del margen de las restricciones establecidas (instalar o borrar software, proveer cualquier servicio etc.). El cumplimiento de las restricciones negociadas especificadas en el reglamento (78) es monitorizado por el módulo de control (77) del entorno básico (5) del CAP. Las restricciones no pueden ser modificadas unilateralmente por una parte (30, 31), si la modificación influye de alguna manera en las restricciones de otras partes (30, 31). Se puede salir (24) del estado "ready" (28), entre otros, en los tres casos que se describen a continuación, y en estos casos se podrá pasar al estado "prepared (27)":

- mediante una solicitud de modificación transmitida por una parte (30, 31) del CAP al módulo de control (77) del entorno básico (5)

- después del vencimiento de un período de validez definido para unas restricciones (duración de uso vencida)

- por la transgresión no autorizada de las restricciones por una parte (30, 31).

Una modificación de las restricciones solamente se puede efectuar mediante una negociación conjunta de las partes (30, 31) cuyos entornos de usuario (3, 4) sean afectados por la modificación. Por este motivo, una modificación de unas restricciones deseadas por una parte (30, 31) del CAP solamente puede ser iniciada por medio de una solicitud de modificación. La parte (30, 31) que desee una modificación de sus restricciones debe transmitir tal solicitud de modificación al módulo de control (77) del entorno básico (5). Si la solicitud de modificación se inicia con éxito, el CAP cambia (24) al estado prepared (27) y permanece (25) en él, hasta que la solicitud de modificación sea tramitada o cancelada.

En el caso de una transgresión no autorizada detectada de las restricciones por una parte (30, 31) se le podrán retirar los derechos de uso a esta parte (30, 31). Con este fin, el propio módulo de control (77) del entorno básico (5) provoca una modificación de las restricciones. Para ello, el CAP cambia (24) al estado prepared (27).

Para las restricciones puede existir un período de validez finito. Después del vencimiento de este período de validez para las restricciones, el propio módulo de control (77) del entorno básico (5) del CAP puede provocar una modificación de las restricciones. El CAP cambia (24) al estado prepared (27).

En resumen, el objeto de la invención es permitir el uso paralelo de un punto de acceso o de una red de estos puntos de acceso por varias partes (30, 31). Por ejemplo, dos o más proveedores utilizan un solo punto de acceso en una localidad para ofrecer mediante el mismo su respectiva red de WLAN.

Por consiguiente, ninguna parte (30, 31) posee ya el predominio sobre el respectivo punto de acceso, sino solamente sobre unas participaciones definidas de este punto de acceso. Para este fin, el punto de acceso se divide en varios entornos. Cada parte (30, 31) solamente tiene el predominio dentro de su entorno, pero no sobre todo el punto de acceso.

Para conseguir una relación de confianza entre las partes (30, 31) para este escenario, ninguna parte (30, 31) debe poseer el predominio sobre la totalidad del punto de acceso. Mediante la invención, se elimina este "supervisor", y todas las modificaciones que afecten a más de un entorno serán decididas en común por las partes afectadas (30, 31). Para ello, la invención describe un procedimiento y una disposición sobre cómo se puede implementar técnicamente este proceso de decisión común.

Un entorno privilegiado (el entorno básico (5)) posee los derechos propiamente dichos del supervisor, pero a los que ninguna de las partes (30, 31) tiene acceso, sino que los que son administrados por un módulo de control (77) neutral con respecto a las partes y un reglamento (78) específico. En el caso de desear unas modificaciones que superen sus derechos propios, las partes (30, 31) comunican con este módulo de control (77) que luego comunica con las otras partes (30, 31) y de esta manera controla el proceso de negociación como un elemento neutral. Solamente en el caso de que todas las partes (30, 31) den su consentimiento al módulo de control (77) con respecto al deseo de modificación de la parte solicitante (30, 31), se implementará la modificación por el módulo de control (77), y en el caso contrario, será rechazada.

REIVINDICACIONES

1. Procedimiento para la formación de una red de acceso basada en diferentes topologías para acceder a una red pública mediante una infraestructura facilitada por uno o varios proveedores para el uso compartido paralelo de varias partes, y que consiste en por lo menos un punto de acceso de red (CAP), **caracterizado** por el hecho de que

- el punto de acceso de red (CAP) contiene por lo menos un entorno de usuario y un entorno básico,

- en un entorno de usuario los derechos de uso de unos recursos, los datos y las unidades de datos así como las funciones de un usuario de dicho punto de acceso de red (CAP) están encapsulados y que el entorno de usuario contiene por lo menos un módulo de comunicación, un módulo de seguridad y un módulo de gestión;

- adicionalmente en el entorno básico están encapsuladas las funciones básicas que operan más allá de los límites de los entornos de usuario encapsulados del punto de acceso de red (CAP) y que el entorno básico (5) contiene por lo menos un módulo de comunicación, un módulo de seguridad, un módulo de control y un reglamento, incluyendo los siguientes pasos:

reparto de los derechos de uso de unos recursos de un punto de acceso de red (CAP) entre varios usuarios con igualdad de derechos según un reglamento a negociar, efectuándose por la parte correspondiente un uso solamente de acuerdo con dicho reparto y sin acceder a los recursos de la otra parte,

reparto de los derechos de uso de unos recursos del punto de acceso de red (CAP) solamente de acuerdo mutuo entre todas las partes cuyo entorno de uso esté afectado por la modificación, mediante un proceso de negociación asegurado, implementándose el reparto solamente mediante las funciones básicas del entorno básico.

2. Procedimiento según la reivindicación 1, **caracterizado** por el hecho de que las funciones básicas encapsuladas en un entorno básico de un punto de acceso de red (CAP) comprenden:

- un reglamento que contiene las restricciones, acuerdos sobre el nivel de servicio, negociados contractualmente entre los usuarios con igualdad de derechos de este punto de acceso de red (CAP),

- unas funciones que soportan el transcurso del proceso para la generación, administración, modificación y borrado de entornos de usuarios según las especificaciones del reglamento,

- unas funciones para la monitorización del cumplimiento de las especificaciones del reglamento, en particular para la monitorización del acceso a los recursos del punto de acceso de red CAP,

- unas funciones de seguridad como una instancia de identificación, autenticación, autorización, monitorización de integridad, codificación, detección de errores y reacción a los errores,

- unas funciones de administración para los sistemas de archivos y

- unas funciones de sistema operativo, incluyendo la provisión de interfaces para el acceso a los recursos de hardware del punto de acceso de red CAP.

3. Procedimiento según la reivindicación 1 o 2, **caracterizado** por el hecho de que sólo se puede acceder a las funciones básicas del entorno básico desde entornos de usuario del mismo punto de acceso de red (CAP) mediante distintas tecnologías de acceso y solamente mediante unas interfaces definidas en base a las especificaciones del reglamento y solamente después de la verificación exitosa de una opción de identificación del usuario que esté realizando el acceso.

4. Procedimiento según una de las reivindicaciones 1 a 3, **caracterizado** por el hecho de que las funciones básicas del entorno básico son configurables o fijas y se realizan mediante técnica de hardware o mediante una combinación de software y hardware.

5. Procedimiento según una de las reivindicaciones 1 a 4, **caracterizado** por el hecho de que los derechos de uso de recursos de un punto de acceso de red (CAP) se reparten, donde el reparto basado en hardware requiere por lo menos un sistema de hardware duplicado físicamente con un componente de gestión común.

6. Procedimiento según una de las reivindicaciones 1 a 5, **caracterizado** por el hecho de que los derechos de uso de recursos de un punto de acceso de red (CAP) se reparten de forma relativa o absoluta.

7. Procedimiento según una de las reivindicaciones 1 a 6, **caracterizado** por el hecho de que una parte puede acceder a su entorno de usuario solamente mediante unas interfaces definidas y mediante unas tecnologías de acceso definidas y solamente después de la verificación de una opción de identificación que pertenece a este entorno de usuario.

8. Procedimiento según una de las reivindicaciones 1 a 7, **caracterizado** por el hecho de que el proceso de negociación está controlado con respecto al estado y que comprende por lo menos los estados idle, prepared y ready.

9. Procedimiento según una de las reivindicaciones 1 a 8, **caracterizado** por el hecho de que una solicitud de modificación por parte de un usuario es aceptada por el punto de acceso de red (CAP) solamente en el caso de que la parte correspondiente se haya autenticado con éxito mediante su opción de identificación y que haya sido declarada autorizada.

10. Procedimiento según una de las reivindicaciones 1 a 9, **caracterizado** por el hecho de que una solicitud de modificación contiene informaciones específicas del usuario, y describe las restricciones que haya que modificar, las nuevas, o las que haya que borrar.

11. Disposición con unos medios para la realización del procedimiento según una de las reivindicaciones 1 a 10, comprendiendo la disposición un punto de acceso de red (CAP) y comprendiendo los recursos del punto de acceso de red (CAP):

- por lo menos una interfaz de red inalámbrica que soporta las tecnologías inalámbricas para facilitar una red inalámbrica,

- por lo menos una interfaz de red con cables o inalámbrica para conectar mediante una conexión de banda ancha con una red adicional,

- un hardware básico, consistente en por lo menos una unidad de cálculo y por lo menos una unidad de almacenamiento,

- por lo menos un sistema operativo, y

- por lo menos un sistema de archivos.

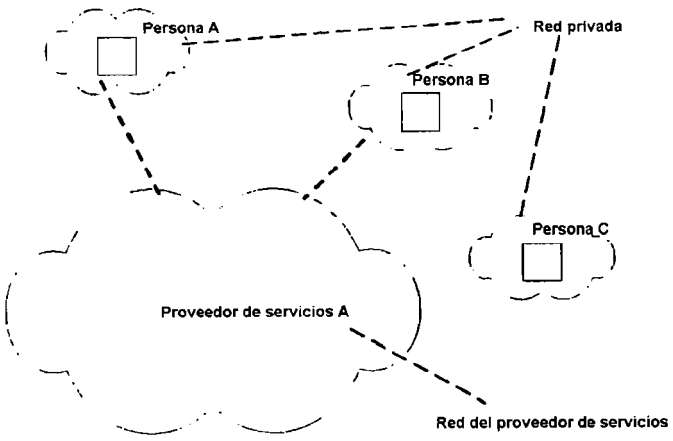
12. Disposición según la reivindicación 11, **caracterizada** por el hecho de que un CAP presenta varias interfaces de red inalámbricas que soportan tecnologías inalámbricas para facilitar una red inalámbrica, y que las interfaces de red soportan las mismas o distintas tecnologías para facilitar una red inalámbrica así como la opción de una gestión dinámica, autónoma de la configuración de radio.

13. Disposición según la reivindicación 11 o 12, **caracterizada** por el hecho de que la interfaz de red inalámbrica o con cables del punto de acceso de red (CAP) soporta cualquier tecnología inalámbrica o con cables para conectar mediante una conexión de banda ancha con una red adicional.

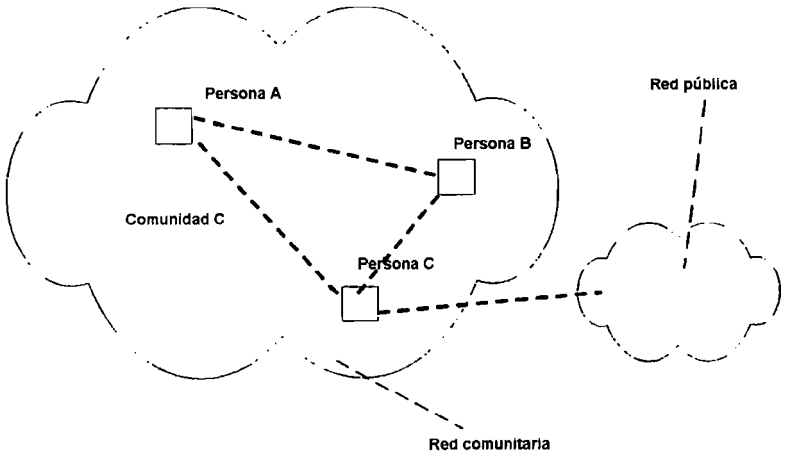
14. Disposición según una de las reivindicaciones 1 a 13, **caracterizada** por el hecho de que los recursos de un punto de acceso de red (CAP) están reunidos dentro de un solo equipo.

15. Disposición según una de las reivindicaciones 1 a 13, **caracterizada** por el hecho de que los recursos de un punto de acceso de red (CAP) están repartidos entre varios equipos, formando un equipo una unidad funcional con recursos e interfaces definidos, respectivamente.

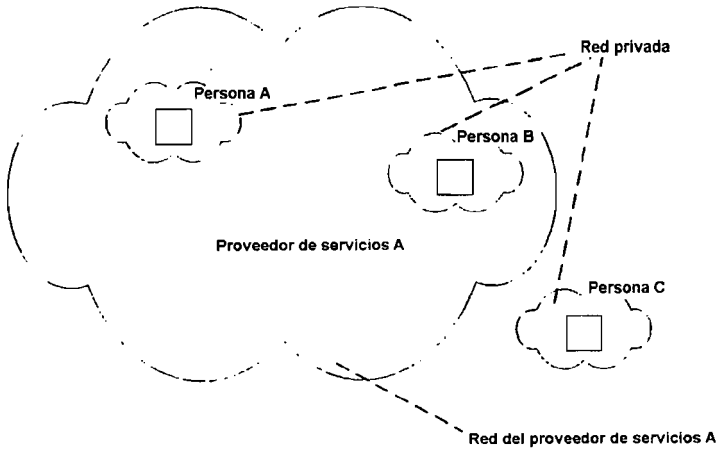
[Fig. 1]



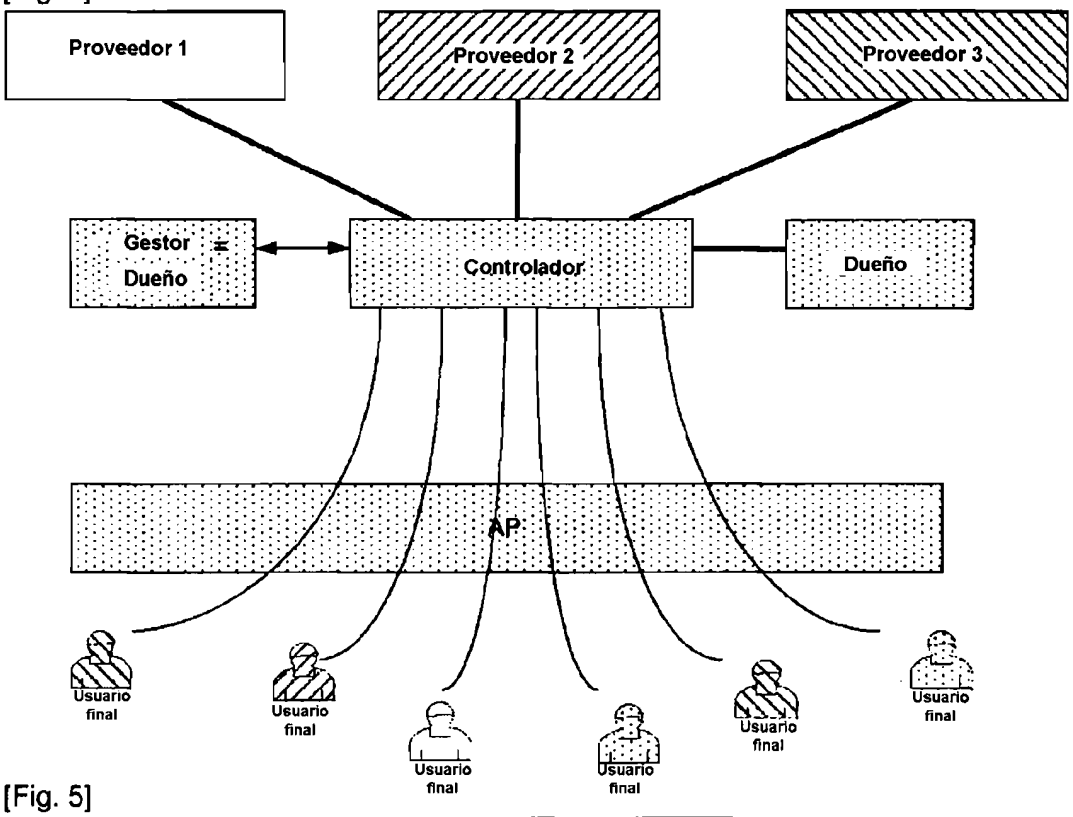
[Fig. 2]



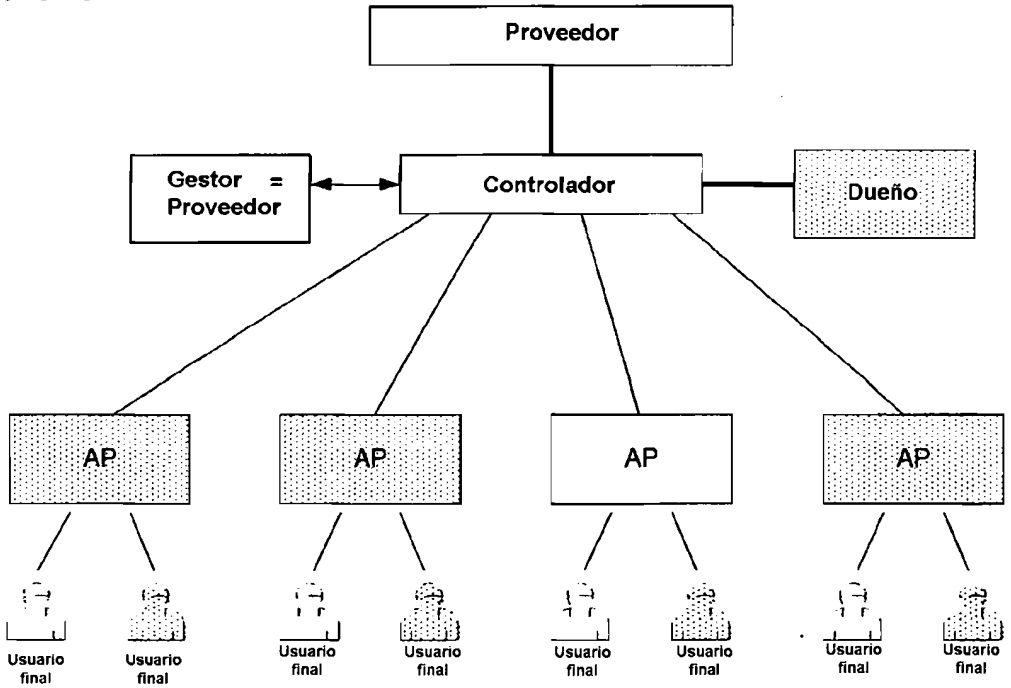
[Fig. 3]



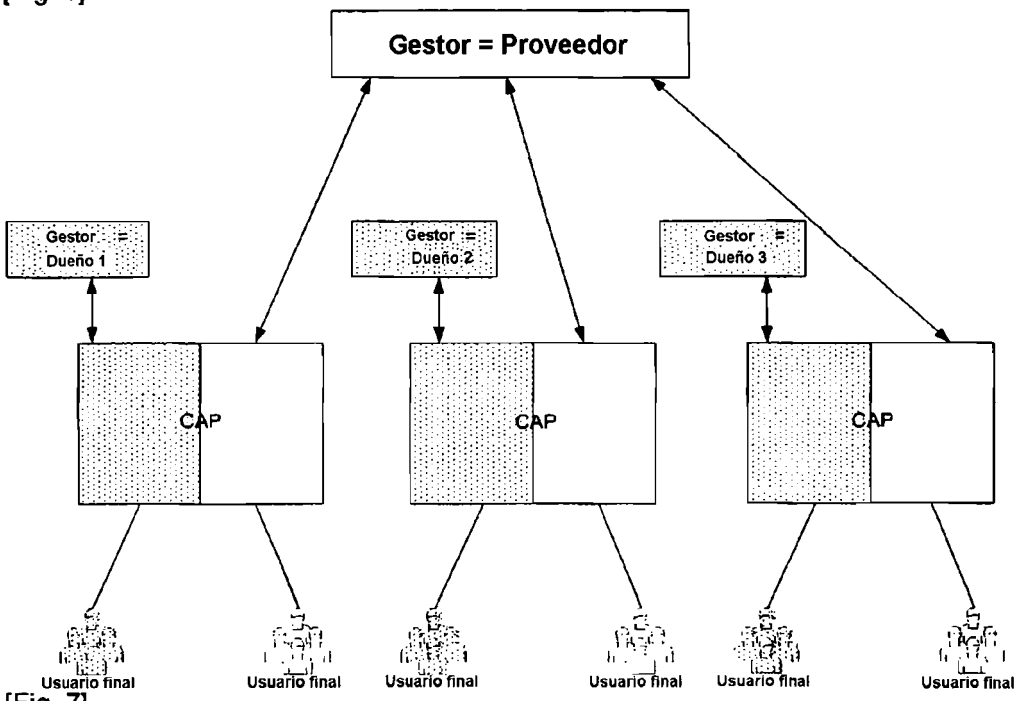
[Fig. 4]


Proveedor 1
Proveedor 2
Proveedor 3
Gestor = Dueño
Controlador
Dueño
AP
Usuario final
Usuario final
Usuario final
Usuario final
Usuario final
Usuario final

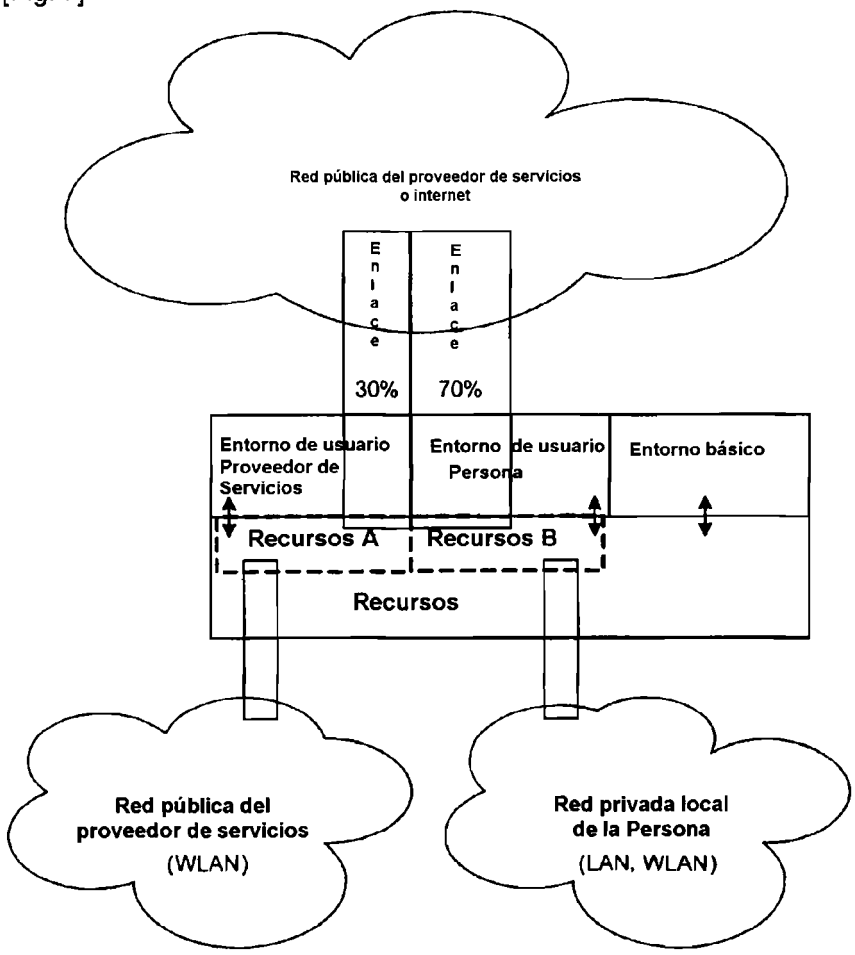
[Fig. 5]


Proveedor
Gestor = Proveedor
Controlador
Dueño
AP
AP
AP
AP
Usuario final
Usuario final
Usuario final
Usuario final
Usuario final
Usuario final
Usuario final
Usuario final

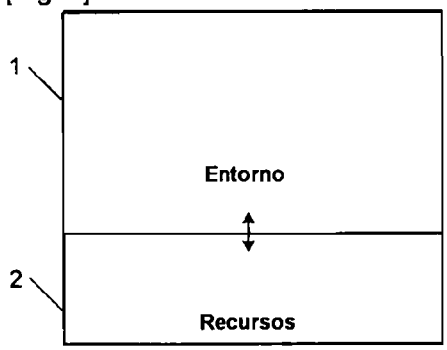
[Fig. 6]


Gestor = Proveedor
Gestor = Dueño 1
Gestor = Dueño 2
Gestor = Dueño 3
CAP
CAP
CAP
Usuario final
Usuario final
Usuario final
Usuario final
Usuario final
Usuario final

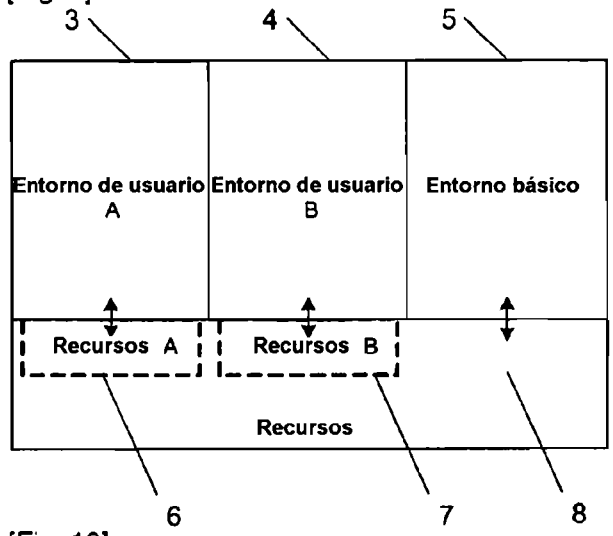
[Fig. 7]


Red pública del proveedor de servicios o internet
Enlace
Enlace
30%
70%
Entorno de usuario Proveedor de Servicios
Entorno de usuario Persona
Entorno básico
Recursos A
Recursos B
Recursos
Red pública del proveedor de servicios (WLAN)
Red privada local de la Persona (LAN, WLAN)

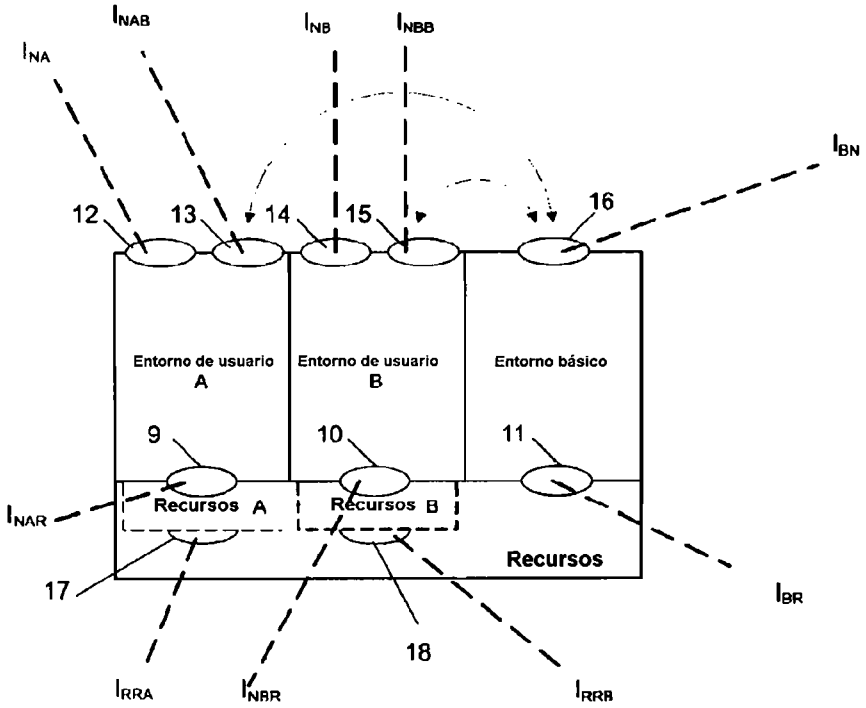
[Fig. 8]



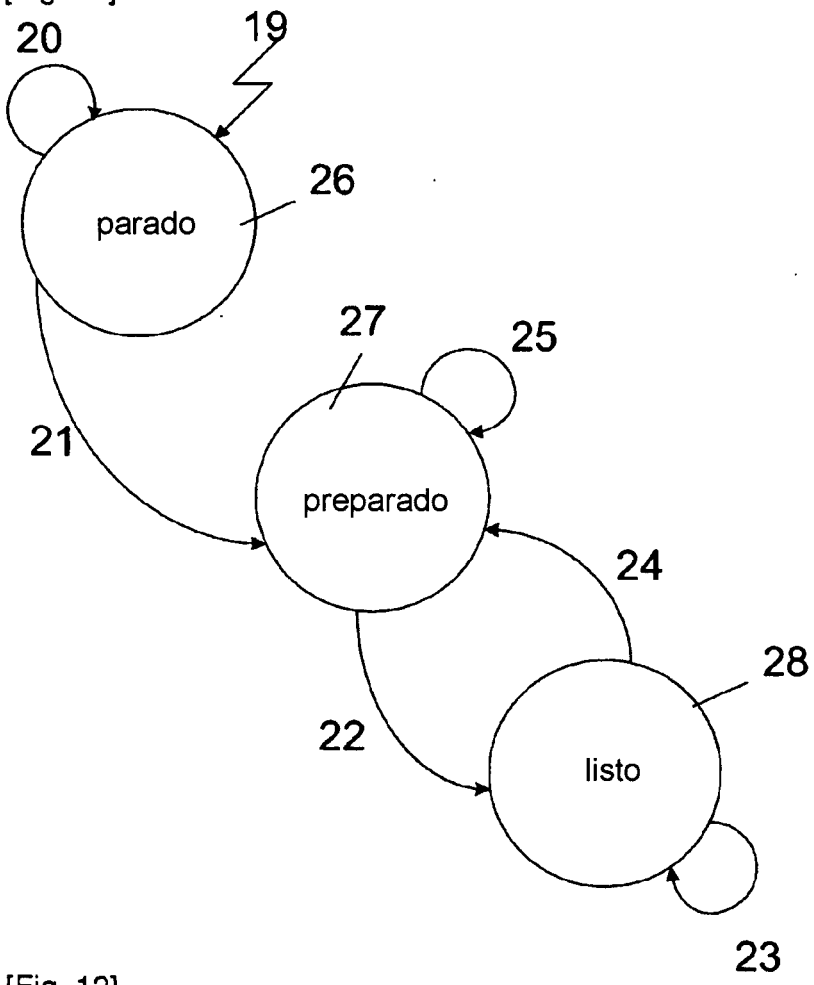
[Fig. 9]



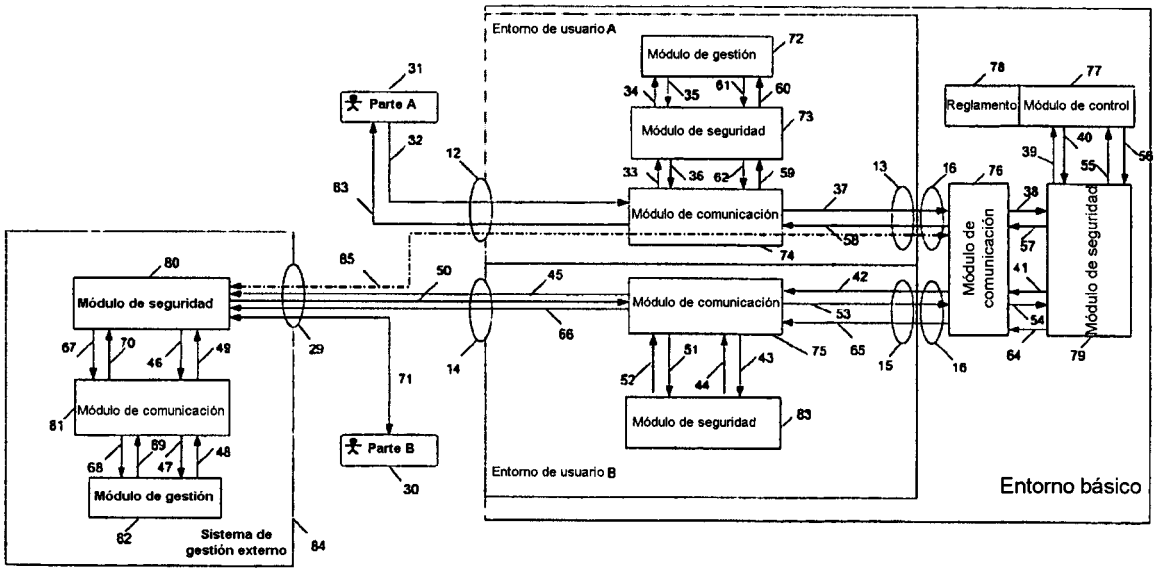
[Fig. 10]



[Fig. 11]


20
19
parado
26
27
25
21
preparado
24
28
22
listo
23

[Fig. 12]


Entorno de usuario A
Módulo de gestión
Parte A
Módulo de seguridad
Módulo de comunicación
Reglamento
Módulo de control
Módulo de comunicación
Módulo de seguridad
Módulo de seguridad
Módulo de comunicación
Módulo de gestión
Sistema de gestión externo
Parte B
Módulo de seguridad
Entorno de usuario B
Entorno básico