

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 421 924**

51 Int. Cl.:

H04W 8/26 (2009.01)

G06F 21/34 (2013.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **29.09.2006** **E 06805952 (6)**

97 Fecha y número de publicación de la concesión europea: **03.04.2013** **EP 2070379**

54 Título: **Servicios para usuarios móviles a través de distintos aparatos electrónicos**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
06.09.2013

73 Titular/es:

TELECOM ITALIA S.P.A. (100.0%)
PIAZZA DEGLI AFFARI, 2
20123 MILANO, IT

72 Inventor/es:

VARRIALE, ANTONIO;
MANGIABENE, SIMONETTA;
ALESSIO, ELISA;
TUROLLA, MAURA y
MARCELLI, MAURIZIO

74 Agente/Representante:

PONTI SALES, Adelaida

ES 2 421 924 T3

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

DESCRIPCIÓN

Servicios para usuarios móviles a través de distintos aparatos electrónicos.

5 CAMPO DE LA INVENCION

[0001] La presente invención se refiere al uso, provisión, personalización y facturación de servicios para usuarios móviles a través de distintos aparatos electrónicos.

10 ANTECEDENTES DE LA INVENCION

[0002] Un usuario móvil, especialmente un usuario móvil por motivos empresariales, tiene a menudo la necesidad de usar diversos servicios, en particular servicios de comunicaciones, a través de distintos aparatos electrónicos de oficina mientras está de viaje o simplemente fuera de su oficina.

15

[0003] Actualmente, necesita diversas suscripciones diferentes (incluso con el mismo proveedor de servicios) para ser capaz de usar y pagar los mismos o similares servicios a través de distintos aparatos electrónicos, tales como ordenadores personales, típicamente en diferentes lugares, por ejemplo en diferentes países.

20 **[0004]** Esto es engorroso tanto dado que requiere una serie de suscripciones como dado que requiere la emisión y el pago de una serie de facturas.

[0005] A partir de la solicitud de patente EP1607906, se conocen un par de tarjetas de autenticación. Una primera tarjeta de autenticación se inserta (instala) en un teléfono celular y una segunda tarjeta de autenticación se inserta (instala) en una PDA. La primera tarjeta de autenticación comprende una unidad de transmisión de un código de identificación y la segunda tarjeta de autenticación comprende una unidad de cancelación de restricción de uso. Las dos unidades intercambian el código de identificación por medio de una señal inalámbrica y autentican el código de identificación mutuamente. En el caso en que la PDA se mueve a más de una distancia predeterminada del teléfono celular y el nivel de recepción de señal desde la unidad de transmisión recibida por la unidad de cancelación es más pequeño que un valor predeterminado (no puede llevarse a cabo una autenticación fiable), o en el caso en que la unidad de cancelación no pueda autenticar el código de identificación de la unidad de transmisión, la unidad de cancelación detiene la transmisión de la señal de cancelación de restricción de uso a la PDA; como resultado, la PDA ya no está en un estado utilizable y el usuario ya no es capaz de usarla.

35 **[0006]** A partir de la solicitud de patente WO0131877, se conoce un método y una disposición en los que cualquier información privada o secreta que es necesaria para autenticación del cliente puede almacenarse en una tarjeta SIM personal específica y usarse en combinación con un teléfono móvil como una pasarela de seguridad a una red interna protegida. Un empleado que se encuentre lejos de su oficina habitual puede, por medio de un teléfono móvil que funciona como una pasarela de seguridad, comunicarse con la red interna protegida de su empleador; el empleado puede usar cualquier anfitrión remoto para acceder a la red interna protegida pero a través de un teléfono móvil provisto de la tarjeta SIM personal específica. La solución es mover la función de seguridad a un teléfono móvil donde está implementada una pasarela de seguridad ligera o cortafuegos. Como alternativa, el empleado puede instalar la tarjeta SIM personal específica directamente en cualquier anfitrión remoto para comunicarse con la red interna protegida.

45

[0007] A partir de la solicitud de patente WOA959360, se conoce una disposición para un sistema de comunicación inalámbrica; esta disposición comprende un terminal de comunicación inalámbrica y una unidad de identidad del abonado que está adaptada para comprender un módulo de identidad del abonado al que se le asigna una identidad del abonado; la unidad de identidad del abonado está dispuesta para comunicar al módulo de identidad del abonado datos relacionados tales como la identidad del abonado con la terminal en un enlace de comunicación inalámbrica local; esta disposición hace posible separar la unidad de identidad del abonado del terminal incluso aunque el terminal esté comunicándose en el sistema inalámbrico; la unidad de identidad del abonado puede hacerse con el control de uno o más terminales de comunicación inalámbrica y se usa para proporcionar autenticación a los terminales.

50

[0008] El documento WO 03/084265 desvela un método y aparato para acceder a una red usando información de identidad del abonado remota. La información de identidad del abonado en una memoria almacenada en un dispositivo tal como un terminal móvil puede ser usada a distancia por un segundo dispositivo independiente, estableciendo un enlace de comunicación local entre los dos terminales. La información de identidad del abonado

55

remota es transferida por el enlace de comunicación local y el terminal de comunicación, que está usando la información de identidad del abonado remota, puede registrarse con la red usando esa información.

[0009] El Solicitante destaca que, en la solución según el documento EP1607906, la autenticación mutua del teléfono celular y la PDA se usa solamente para permitir el uso de la PDA por el usuario.

[0010] En la solución según el documento W00131877, es necesario usar la tarjeta SIM personal específica, instalarla en un teléfono o un ordenador, para ser capaz de acceder a una red interna por medio de este ordenador.

10 **[0011]** En la solución según el documento W09959360, el funcionamiento del terminal o terminales de comunicación inalámbrica requiere la presencia y el funcionamiento activo de la unidad de identidad del abonado y el módulo de identidad del abonado asociado durante la comunicación; de hecho, ninguno de los terminales de comunicación está provisto de un módulo de identidad del abonado asociado. Por lo tanto, esta solución requiere terminales de comunicación específicos para ser implementada.

15 **[0012]** Tal como ya se ha dicho, el Solicitante ha observado que un usuario móvil tiene la necesidad de usar los mismos o similares servicios a través de distintos aparatos electrónicos.

20 **[0013]** Adicionalmente, el Solicitante ha observado que un usuario móvil tiene también la necesidad de tener estos servicios personalizados de la misma o similar manera. La facturación de estos servicios debe ser segura y fiable; esto es especialmente importante cuando los aparatos electrónicos son usados por diferentes usuarios y aún más cuando están en un sitio público, por ejemplo un hotel o un avión.

25 **[0014]** Finalmente, existe una necesidad de soluciones que requieran el cambio mínimo con respecto a los sistemas y aparatos existentes.

[0015] Es el objeto de la presente invención satisfacer al menos parte de estas necesidades.

RESUMEN DE LA INVENCION

30 **[0016]** El Solicitante ha considerado tener una primera tarjeta inteligente adaptada para transferir información de identificación del abonado y posiblemente información de autenticación del abonado almacenada en su interior a otras tarjetas inteligentes asociadas con aparatos electrónicos, de modo que puedan usarla para usar o proporcionar servicios de forma autónoma con respecto a la primera tarjeta inteligente. De esta manera, gracias a una única
35 tarjeta inteligente (es decir, una única suscripción y un único proceso de facturación y de pago) los mismos o similares servicios, en particular servicios de comunicación, pueden usarse o proporcionarse a través de distintos aparatos electrónicos.

40 **[0017]** Típicamente esta primera tarjeta inteligente, llamada "tarjeta maestra" o tarjeta del abonado, se instala en un terminal de telefonía móvil, por ejemplo un teléfono celular.

[0018] Típicamente, la otra tarjeta inteligente, llamada "tarjeta esclava" o tarjeta del aparato se instala en un aparato electrónico, por ejemplo un ordenador personal.

45 **[0019]** La presente invención permite ventajosamente la transferencia, en particular desde la tarjeta maestra a la tarjeta esclava, no solamente de información de identificación del abonado sino también de información de los derechos del abonado y/o información del crédito del abonado y/o información de las preferencias del abonado y/o aplicaciones y/o comandos de aplicación.

50 **[0020]** La comunicación entre las dos tarjetas inteligentes puede ser directa, fiable y segura por medio de una tecnología inalámbrica segura tal como ZigBee™. De esta manera, mejora la seguridad dado que la fuente de transmisión es segura, dado que puede ser un módulo seguro implementado a través de una tarjeta inteligente, el destino de transmisión es seguro, dado que puede ser un módulo seguro implementado a través de una tarjeta inteligente, y el canal de comunicación (o transmisión) es seguro. La expresión tarjeta inteligente identifica en el
55 presente documento en general una tarjeta que tiene funcionalidades de procesamiento y, preferentemente, propiedades resistentes a la manipulación, por ejemplo un criptoprocador seguro y un sistema de archivos seguro.

[0021] La presente invención proporciona un método de provisión de servicios que comprende las etapas de:

A) proporcionar un aparato electrónico asociado a una tarjeta del aparato y capaz de proporcionar un servicio por medio de información de identificación,

5 B) proporcionar un terminal de telefonía móvil,

C) asociar una tarjeta del abonado que almacena información de identificación del abonado con el terminal de telefonía móvil,

10 D) transferir al menos la información de identificación del abonado desde la tarjeta del abonado a la tarjeta del aparato cuando el terminal de telefonía móvil está en las proximidades del aparato electrónico,

E) almacenar la información transferida en la tarjeta del aparato, y

15 F) proporcionar el servicio por medio de la información transferida.

[0022] Preferentemente, dicho método comprende además la etapa de:

20 G) proporcionar al aparato electrónico un detector de proximidad de radio asociado a un espacio de cobertura de radio y adaptado para detectar un terminal de telefonía móvil cuando está dentro del espacio de cobertura de radio.

[0023] Preferentemente, la tarjeta del abonado y la tarjeta del aparato comprenden, cada una, una unidad de comunicación por radio para comunicarse conjuntamente.

25 **[0024]** Preferentemente, dicho método comprende además la etapa de:

H) eliminar o inhabilitar la información transferida cuando el terminal de telefonía móvil está fuera de las proximidades del aparato electrónico.

30 **[0025]** Preferentemente, la etapa D permite transferir también información de autenticación del abonado

[0026] Preferentemente, dicho método comprende además la etapa de:

35 N) transferir aplicaciones desde el aparato electrónico al terminal de telefonía móvil, y

O) almacenar las aplicaciones transferidas en el terminal de telefonía móvil.

40 **[0027]** Preferentemente, las aplicaciones transferidas se almacenan en la tarjeta del abonado asociada o se pasan a través de la tarjeta del abonado asociada.

[0028] Según otro aspecto, la presente invención proporciona una tarjeta inteligente para uso en comunicaciones adaptada para insertarla en un terminal de telefonía móvil según la reivindicación 9.

45 **[0029]** Preferentemente, el bloque de configuración está adaptado para transmitir también información de autenticación del abonado y/o información de los derechos del abonado y/o información del crédito del abonado y/o información de las preferencias del abonado a la tarjeta inteligente del aparato electrónico remoto.

50 **[0030]** Preferentemente, la tarjeta inteligente comprende un bloque de programación adaptado para transmitir aplicaciones a la tarjeta inteligente del aparato electrónico remoto.

[0031] Según otro aspecto, la presente invención proporciona una tarjeta inteligente para uso en comunicaciones adaptada para insertarla en un aparato electrónico local según la reivindicación 12.

55 **[0032]** Preferentemente, el bloque de configuración está adaptado para recibir también información de autenticación del abonado y/o información de los derechos del abonado y/o información del crédito del abonado y/o información de las preferencias del abonado desde la tarjeta inteligente del aparato electrónico remoto.

[0033] Preferentemente, la tarjeta inteligente comprende un bloque de programación adaptado para recibir aplicaciones desde la tarjeta inteligente del aparato electrónico remoto.

[0034] Preferentemente, la tarjeta inteligente tiene al menos dos modos de funcionamiento, en un primer modo de funcionamiento que usa información de identificación del abonado almacenada previamente a nivel local y en un segundo modo de funcionamiento que usa información de identificación del abonado recibida a distancia.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0035] La presente invención se volverá más evidente a partir de la siguiente descripción que se considerará junto con los dibujos adjuntos, en los que:

La figura 1 muestra esquemáticamente un sistema según la presente invención,

La figura 2 muestra un diagrama de bloques esquemático de parte del sistema de la figura 1, y

La figura 3 muestra una posible separación del software en tarjetas inteligentes según la presente invención.

[0036] Debe entenderse que la siguiente descripción y los dibujos adjuntos no deben ser interpretados como limitaciones de la presente invención sino simplemente como ejemplificaciones.

DESCRIPCIÓN DETALLADA DE LA INVENCION

[0037] En la figura 1, todo el sistema se indica con la referencia 100. El sistema 100 comprende:

- una red de telecomunicaciones 110, por ejemplo una red 2G/3G, tal como GSM y/o UMTS;
- un terminal de telefonía móvil 120, por ejemplo un teléfono móvil de tecnología 2G para intercambiar llamadas telefónicas;
- una primera tarjeta inteligente 130, específicamente una tarjeta “maestra”, que tiene una unidad de comunicación por radio integrada;
- un aparato electrónico 150, por ejemplo, un aparato electrónico de oficina, por ejemplo un PC portátil que tiene un dispositivo para intercambiar e-mails (así como para navegar por Internet) por medio de una conexión de tecnología 3G; y
- una segunda tarjeta inteligente 140, específicamente una tarjeta “esclava”, que tiene una unidad de comunicación por radio integrada.

[0038] Para simplificar la descripción de la presente invención, el escenario mostrado en la figura 1 se reduce a su mínimo, es decir un terminal de telefonía móvil y un aparato electrónico de oficina. De todos modos, en general, puede haber muchos aparatos electrónicos: de hecho, tal como ya se ha explicado anteriormente, un usuario móvil tiene la necesidad de usar los mismos o similares servicios (en el ejemplo de la figura 1 por ejemplo intercambio de e-mails y/o conexión a Internet) a través de distintos aparatos electrónicos de oficina. En un caso general, puede haber una pluralidad de aparatos electrónicos de oficina y una pluralidad de terminales de telefonía móvil.

[0039] Las tarjetas inteligentes 130 y 140 pueden tener la arquitectura y el funcionamiento interno desvelados por ejemplo en las solicitudes de patente W02005104584 y WO2006056220 del mismo Solicitante.

[0040] En la realización de la figura 1, la tarjeta inteligente 130 tiene todas las funcionalidades de una tarjeta SIM [Módulo de Identificación del Abonado] y funcionalidades adicionales que se describirán a continuación; aunque la tarjeta inteligente 140 tiene todas las funcionalidades de una tarjeta USIM [SIM Universal] y funcionalidades adicionales que se describirán a continuación. Las funcionalidades de SIM o USIM preferentemente comprenden funcionalidades de autenticación del operador de red.

[0041] Las unidades de comunicación por radio de tarjetas inteligentes 130 y 140 son del tipo de (relativamente) corto alcance; en otras palabras, están adaptados para las llamadas aplicaciones WPAN [Red de Área Personal Inalámbrica]; por ejemplo usan la tecnología estándar ZigBee™. Esta tecnología es particularmente adecuada para la presente invención debido al tipo de información transmitida y recibida por las tarjetas inteligentes, es decir, secreta, como por ejemplo en particular la clave KI y/o el código IMSI, dado que implementa un canal de

comunicación seguro. Como alternativa, estas unidades de comunicación por radio pueden usar, por ejemplo, la tecnología estándar Bluetooth™. Estas tecnologías permiten detectores de proximidad de radio asociados a un espacio de cobertura de radio que pueden ser programables.

5 **[0042]** Debe observarse que la seguridad puede ser intrínseca al protocolo de comunicación entre las tarjetas inteligentes o puede implementarse, por ejemplo, a nivel de la aplicación.

[0043] La tarjeta inteligente 130, como cualquier tarjeta SIM, almacena de forma segura información de identificación del abonado e información de autenticación del abonado.

10

[0044] Para GSM, la información de identificación comprende un código IMSI [Identidad Internacional del Abonado a un Móvil] y la información de autenticación comprende una clave KI [Clave Individual de Autenticación del Abonado]; debe observarse que, aunque el código IMSI no es secreto (incluso aunque se recomiende limitar su circulación por redes de comunicación), la clave KI es secreta y es conocida solamente por la tarjeta SIM (eso, según la técnica anterior, la mantiene internamente protegida) y por el proveedor de servicios (que expidió esta tarjeta SIM).

15

[0045] La información de identificación del abonado se usa para identificar al abonado que está interesado en usar el servicio y al que se le debe facturar.

20

[0046] La tarjeta inteligente 140, como cualquier SIM o USIM, permite tanto el uso de un servicio de comunicación desde la red de telecomunicaciones como la provisión de un servicio de comunicación correspondiente a un usuario en base a un código ISMI y una clave KI.

25 **[0047]**

Según la presente invención, se definen capacidades “maestra” y “esclava”:

- Maestra: tarjeta inteligente asociada al abonado, que se insertará en el terminal de telefonía móvil: y
- Esclava: tarjeta inteligente asociada al aparato que proporciona el servicio, que se insertará en el aparato electrónico de oficina, configurable y programable por una tarjeta maestra.

30

[0048] En la realización de la figura 1, dicha configuración y programación se lleva a cabo a través de un canal de comunicación por radio de proximidad 30 implementado gracias a las unidades de comunicación por radio de las dos tarjetas inteligentes.

35

[0049] En la realización de la figura 1, la tarjeta esclava 140 puede estar configurada por la tarjeta maestra 130 en términos de identificación del abonado, autenticación del abonado, derechos del abonado, crédito del abonado y preferencias del abonado. La tarjeta esclava 140 puede ser programada por la tarjeta maestra 130 en términos de aplicaciones que serán ejecutadas típicamente en el aparato electrónico de oficina asociado. La tarjeta maestra 140 también puede preguntar a la tarjeta esclava 130 sobre las funcionalidades que el aparato asociado a ella es capaz de exportar; en este caso, por ejemplo, el terminal de telefonía móvil 120, a través de la tarjeta maestra 130, podría ser capaz de controlar y/o ejecutar a distancia, a través de la tarjeta esclava 140, aplicaciones residentes en el aparato electrónico de oficina 150.

40

[0050] El sistema 100 de la figura 1 incluye dos tipos de canales de comunicación por radio. El primero es un canal de radio de proximidad 30, que es el canal de radio entre las tarjetas 130 y 140. El segundo es una canal de radio de amplio alcance; para fines de claridad, el canal entre la red 110 y el terminal de telefonía móvil 120 se indica con la referencia 10, mientras que el canal entre la red 110 y el aparato electrónico de oficina 150 se indica con la referencia 20. Debe observarse que, aunque el canal entre la red y el terminal de telefonía móvil tiene que ser de tipo de radio de amplio alcance, el canal de comunicación asociado al aparato electrónico de oficina puede ser de tipo por cable (basado por ejemplo en cable eléctrico o fibra óptica) o de tipo inalámbrico (es decir por radio) o de tipo mixto y puede ser para conexión a la misma o una red diferente con respecto a la red de telecomunicaciones asociada al terminal de telefonía móvil.

50

[0051] La tarjeta maestra 130 y la tarjeta esclava 140 están conectadas respectivamente al terminal de telefonía móvil 120 y al aparato electrónico de oficina 150 a través de una interfaz de comunicación, por ejemplo tanto a través de la interfaz estándar ISO7816 conocida. Para fines de claridad, las dos interfaces de comunicación se indican con dos referencias diferentes, respectivamente 40 y 50; de hecho, en general, pueden ser diferentes y/o según la memoria descriptiva patentada; esto se aplica especialmente para la interfaz 50 entre la tarjeta esclava 140

55

y el aparato 150.

[0052] Según la descripción anterior, el sistema 100 proporciona dos tarjetas inteligentes 130 y 140 que implementan, cada una, un módulo seguro, específicamente un Módulo de Identificación del Abonado.

[0053] Como alternativa, una o ambas de ellas pueden realizarse a través de una tarjeta SDIO [Entrada/Salida Digital Segura] o un adaptador USB [Bus Universal en Serie] y una interfaz correspondiente en el aparato; esta solución es particularmente aplicable al aparato electrónico de oficina. Según una implementación preferida de esta alternativa, la tarjeta SDIO/adaptador USB tiene una unidad de comunicación por radio de proximidad integrada preferentemente con los elementos descritos anteriormente, es decir que usa tecnología ZigBee™ o Bluetooth™.

[0054] De todos modos, de hecho es posible que el módulo seguro y/o la unidad de comunicación por radio de proximidad asociada esté integrado en el aparato; esta solución es particularmente aplicable al aparato electrónico de oficina. Incluso en este caso, las dos tecnologías de comunicación preferidas son ZigBee™ o Bluetooth™.

[0055] Sea cual sea la implementación del módulo o módulos seguros, la arquitectura del hardware y la arquitectura del software correspondientes son básicamente las mismas.

[0056] Los componentes del sistema 100 interactúan apropiadamente entre sí y, de esta manera, un usuario puede usar servicios proporcionados por el aparato electrónico de oficina 150 gracias a la información de identificación del abonado y posiblemente la información de autenticación del abonado almacenada en la tarjeta maestra 130 y transferida al aparato electrónico de oficina 150, particularmente a la tarjeta esclava 140; por otro lado, el aparato electrónico de oficina 150 proporciona al usuario servicios según su propias capacidades y gracias a la información de identificación del abonado y posiblemente la información de autenticación del abonado almacenada en la tarjeta maestra 130 y recibida de ésta. En el caso de un servicio de comunicación, el aparato electrónico de oficina 150 usa un servicio de comunicación proporcionado por un proveedor de servicios por medio de la información de identificación y autenticación del abonado transferida y, a su vez, proporciona un servicio de comunicación al usuario. Para estos fines, el aparato electrónico de oficina 150 puede necesitar no solamente información de identificación del abonado, sino también información de los derechos del abonado y/o información del crédito del abonado; dicha información adicional se almacena típicamente en una tarjeta del abonado, como por ejemplo una tarjeta SIM y, en la realización de la figura 1, se almacena en la tarjeta maestra 130 y se transfiere a la tarjeta esclava 140 a través del canal de comunicación por radio de proximidad 30.

[0057] El aparato electrónico de oficina 150 puede ser capaz de personalizar los servicios proporcionados al usuario, para este fin, necesita información de las preferencias del abonado; la información de las preferencias del abonado se almacena típicamente en una tarjeta del abonado, como por ejemplo una tarjeta SIM y, en la realización de la figura 1, se almacena en la tarjeta maestra 130 y se transfiere a la tarjeta esclava 140 a través del canal de comunicación por radio de proximidad 30.

[0058] Debe entenderse que la transferencia de la información del abonado tiene lugar cuando el terminal de telefonía móvil está en las proximidades del aparato electrónico de oficina, más específicamente cuando entra en su espacio de cobertura de radio. La información del abonado transferida se almacena en el aparato electrónico de oficina, particularmente en la tarjeta esclava asociada 140, para ser usada posteriormente una o más veces por el aparato electrónico de oficina para usar y/o proporcionar servicios independientemente de la tarjeta maestra 130. Dicho almacenamiento puede ser temporal o permanente; en el caso temporal, al almacenamiento puede comenzar cuando el terminal de telefonía móvil entra en las proximidades del aparato electrónico de oficina, más específicamente cuando entra en su espacio de cobertura, y puede terminar cuando el terminal de telefonía móvil abandona las proximidades del aparato electrónico de oficina, más específicamente cuando sale de su espacio de cobertura; el final del almacenamiento puede corresponder a la eliminación (es decir supresión o borrado) de la información transferida desde medios de almacenamiento o a su inhabilitación (por ejemplo marcando la información almacenada como no accesible o no utilizable).

[0059] Debe observarse que, en la realización de la figura 1, la transferencia de información tiene lugar directamente entre las dos tarjetas inteligentes; de todos modos, en realizaciones alternativas la transferencia de información entre las dos tarjetas inteligentes puede tener lugar a través del terminal de telefonía móvil y el aparato electrónico de oficina, por ejemplo, a través de una comunicación directa entre el terminal de telefonía móvil y el aparato electrónico de oficina.

[0060] A continuación se proporcionará un ejemplo para explicar el procedimiento de configuración junto con un servicio de comunicación.

5 **[0061]** Consideremos, por ejemplo, un PC portátil compartido por muchos usuarios, con módem UMTS/HSDPA [Sistema Universal de Telecomunicaciones Móviles / Acceso de Alta Velocidad a Paquetes en Enlace Descendente] integrado. En este caso la conexión a Internet es el servicio proporcionado por el aparato electrónico de oficina al usuario y la conexión de red UMTS/HSDPA es el servicio de comunicaciones usado por el aparato electrónico de oficina para proporcionar el servicio de conexión a Internet al usuario. Para ser identificado y
10 autenticado por la Red, es necesario que una tarjeta del abonado está asociada con el PC portátil.

[0062] Según la técnica anterior, para gestionar una única suscripción (para comodidad tanto del operador como del usuario), un usuario tiene que extraer su tarjeta del abonado, por ejemplo una tarjeta SIM o USIM, de su teléfono móvil e insertarla en el PC portátil; esta operación es engorrosa; adicionalmente, de esta manera, ya no
15 puede usar su teléfono móvil.

[0063] La presente invención permite proyectar temporalmente la información del abonado, en particular información de identidad del abonado y posiblemente información de autenticación del abonado, de la tarjeta maestra 130, que permanece dentro del teléfono móvil, en la tarjeta esclava 140, instalada dentro del PC portátil, de modo que el PC portátil es capaz de acceder a la Red, sin quitar ninguna tarjeta; esta proyección se lleva a cabo a través del canal de comunicación por radio de proximidad 30. Típicamente, dicha proyección comienza cuando el teléfono móvil 120 y la tarjeta maestra asociada 130 entran en el espacio de cobertura de radio de la tarjeta esclava 140, continúa durante el periodo de cobertura, y termina cuando el teléfono móvil 120 y la tarjeta maestra asociada 130 salen del espacio de cobertura de radio de la tarjeta esclava 140.
20

[0064] El procedimiento de identificación/autenticación con la Red podría implementarse por ejemplo en dos fases. En una primera fase, la información de identificación permanentemente almacenada en la tarjeta esclava 140 se usa para identificar y autenticar solamente el PC portátil como un "aparato de oficina de confianza", es decir "de confianza" para la Red y/o su Operador. En una segunda fase, la tarjeta maestra 130 proyecta al menos su información de identificación y autenticación del abonado (pero posiblemente también información de crédito y/o derechos y/o preferencias del abonado) en la tarjeta esclava 140 y el aparato electrónico de oficina la usa para identificar y autenticar al abonado; seguidamente el Operador puede comenzar el procedimiento de facturación. Es evidente que, de esta manera, la facturación se unifica incluso aunque puedan aplicarse diferentes cargos cuando el mismo abonado usa un terminal de telefonía móvil o un aparato electrónico de oficina.
25

[0065] Dado que la comunicación entre los dos módulos seguros es a través de un canal seguro (implementado a través de tecnología inalámbrica ZigBee™), la seguridad tanto para la información de identificación del abonado como para la información de autenticación del abonado está completamente garantizada. En particular, la seguridad del canal está garantizada por encriptado de los paquetes de datos en el enlace de radio a nivel físico. Dicho encriptado puede obtenerse, por ejemplo, por medio de claves simétricas distribuidas previamente a los módulos seguros, o por medio de claves de sesión generadas de forma dinámica a partir de certificados digitales.
30

[0066] Dado que no se extrae ninguna tarjeta de ningún aparato, en principio ambos aparatos podrían usarse al mismo tiempo; esto tiene sentido dado que un usuario puede tener la necesidad, por ejemplo, de realizar o recibir una llamada telefónica mientras está navegando por Internet o comprobando sus e-mails. De todos modos, esto es una cuestión de la política de servicios por un lado y de limitaciones técnicas por el otro; de hecho, en el ejemplo de la figura 1, la Red debe ser capaz de tratar al mismo tiempo con dos aparatos distintos asociados al mismo abonado. Una solución más sencilla sería que una tarjeta maestra que ha proyectado su información de identificación del abonado a una tarjeta esclava ya no sea capaz de usar su información de identificación del abonado hasta que la proyección haya terminado.
35

[0067] A continuación se proporcionará otro ejemplo para explicar el procedimiento de configuración junto con otro tipo de servicio, concretamente un servicio de seguridad proporcionado por el aparato electrónico de oficina al usuario para datos personales y/o aplicación almacenada en un dispositivo de almacenamiento, por ejemplo un disco duro, del aparato electrónico de oficina.
40

[0068] En este caso, la tarjeta esclava dentro del PC portátil puede estar configurada por la tarjeta maestra dentro del teléfono móvil para permitir a un usuario leer y/o escribir datos personales y/o ejecutar aplicaciones personales; esto puede incluir encriptado/desencriptado.

[0069] La tarjeta maestra proyecta temporalmente información del abonado, en particular información de identidad del abonado tal como una contraseña de acceso del abonado y/o una clave de encriptado/desencriptado, en la tarjeta esclava y el PC portátil asociado a la tarjeta esclava usa esta información para acceder a datos personales y aplicaciones por ejemplo bloqueando/desbloqueando de forma dinámica todo el sistema de archivos o archivos individuales, y/o para encriptar/desencriptar datos personales y aplicaciones. También en este caso y para aumentar la seguridad, puede proporcionarse la transferencia de información de autenticación del abonado.

[0070] Según una característica adicional, el acceso a los datos personales y/o aplicaciones protegidas almacenadas en el PC portátil no solamente puede llevarse a cabo por medio de la información del abonado almacenada en la tarjeta maestra asociada al teléfono móvil, sino que también puede realizarse a distancia por el usuario a través del teléfono móvil por medio del canal de comunicación (por ejemplo seguro) entre la tarjeta maestra y la tarjeta esclava.

[0071] En los ejemplos descritos, la tarjeta esclava es una proyección temporal de la tarjeta maestra; en otras palabras, la tarjeta maestra configura la tarjeta esclava. Dicha proyección/configuración puede aplicarse a todas las funciones llevadas a cabo por la tarjeta esclava o solamente a algunas de ellas; En el último caso, la tarjeta esclava lleva a cabo algunas funciones independientemente de la proximidad a una tarjeta maestra. Puede ser apropiado posibilitar que una tarjeta maestra no proyecte toda la información de configuración (información de identificación, autenticación, crédito, derechos y preferencias del abonado) sino solamente aquellas que es probable que sean útiles o necesarias para un aparato electrónico de oficina asociado a una tarjeta esclava.

[0072] La presente invención posibilita ventajosamente que la tarjeta maestra no solamente configure sino que también programe la tarjeta esclava; esto se usa para añadir (es decir almacenar) aplicaciones (y por lo tanto funcionalidades) adicionales a la tarjeta esclava o al aparato electrónico de oficina asociado a ella.

[0073] Por ejemplo, considerando el sistema 100 donde la tarjeta esclava 140 ya es capaz de permitir algunos servicios al usuario, sin la proximidad a la tarjeta maestra 130. Para el PC portátil de empresa 150 ubicado en una zona común como la sala de reuniones de una Compañía, la tarjeta esclava 140 contiene información relacionada con todos los empleados de la Compañía, como direcciones de e-mail, números de teléfono internos, etc.; de esta manera, cualquier empleado puede enviar e-mails y realizar llamadas telefónicas internas a través del PC portátil 150.

[0074] Cada directivo de la compañía tiene su propia tarjeta maestra que almacena aplicaciones relacionadas con el directivo. Cuando una de estas tarjetas maestras está en las proximidades de la tarjeta esclava, añade temporalmente nuevas funcionalidades al aparato electrónico de oficina a través de la tarjeta esclava cargando nuevas aplicaciones, específicamente las aplicaciones relacionadas con el directivo. Por ejemplo, después de dicha programación, el aparato electrónico de oficina a través de la tarjeta esclava se vuelve capaz de decodificar mensajes secretos o e-mails dirigidos al directivo asociado. Este nuevo servicio no estaba disponible antes del procedimiento de programación de la tarjeta maestra, y no estará disponible tampoco cuando la tarjeta maestra esté fuera del alcance de proximidad.

[0075] La presente invención posibilita ventajosamente que el acoplamiento de la tarjeta maestra y la tarjeta esclava permita al terminal de telefonía móvil controlar y/o usar a distancia las funcionalidades del aparato electrónico de oficina.

[0076] Consideremos una aplicación que permite proyectar por ejemplo presentaciones durante, por ejemplo, una reunión de empresa. En este caso, la tarjeta esclava podría exportar al terminal de telefonía móvil, a través de la tarjeta maestra, el control remoto de la presentación. El usuario será capaz de enviar desde el terminal de telefonía móvil al aparato electrónico de oficina comandos tales como "Siguiente Foto", "Foto Anterior" e "Ir a la Foto". Adicionalmente, el terminal de telefonía móvil podría ser usado para mostrar la interfaz hombre-máquina de la aplicación.

[0077] Desde el punto de vista arquitectónico del hardware, la tarjeta maestra 130 y la tarjeta esclava 140 pueden ser similares y las diferentes funcionalidades pueden estar asociadas a diferente firmware solamente; de todos modos, éste no es siempre el caso para todas las realizaciones de la presente invención.

[0078] Puede estar previsto que la misma tarjeta pueda actuar como maestra en ciertas situaciones y como esclava en otras situaciones; ésta es una razón más para tener la misma arquitectura de hardware o incluso

exactamente el mismo hardware.

[0079] Tal como se muestra en la realización de la figura 2, la tarjeta maestra 130 es capaz de configurar (flecha 341), programar (flecha 342) y enviar comandos (flecha 343) a la tarjeta esclava 140.

[0080] La pila de middleware de la tarjeta maestra está compuesta por un gestor de aplicaciones 300 que gestiona aplicaciones locales (a la tarjeta) 340 y aplicaciones externas (a la tarjeta) 360 y 370 que están típicamente en el terminal de telefonía móvil 120; las aplicaciones 360 interactúan directamente con el gestor de aplicaciones 300 mientras que las aplicaciones 370 interactúan indirectamente con el gestor de aplicaciones 300 a través de una capa de aplicaciones internas (a la tarjeta) 350.

[0081] Las solicitudes de aplicación en el terminal de telefonía móvil 120 pueden traducirse en diferentes procesos que son gestionados por tres bloques específicos 310, 320, 330 en la tarjeta maestra 130. El primer bloque es el bloque emisor de configuraciones 310, que está adaptado para transferir información del abonado (por ejemplo identificación y/o derechos y/o crédito y/o preferencias) desde la tarjeta maestra a la tarjeta esclava. El segundo bloque es un bloque emisor de programas 320, que está adaptado para transferir aplicaciones desde la tarjeta maestra a la tarjeta esclava. El tercer bloque es un bloque emisor de comandos 330, que está adaptado para enviar comandos, típicamente comandos de aplicaciones, desde la tarjeta maestra a la tarjeta esclava; el tercer bloque también puede estar adaptado para recibir respuestas a estos comandos y es por esto que la flecha 343 es bidireccional.

[0082] Las flechas 341, 342, 343 representan flujos de datos entre el teléfono móvil 120 y el aparato electrónico de oficina 150, más particularmente entre la tarjeta maestra 130 y la tarjeta esclava 140. Estos flujos de datos están implementados a través del canal de comunicación por radio de proximidad 30 ventajosamente basado en tecnología ZigBee™.

[0083] En el aparato electrónico de oficina 150, específicamente en la tarjeta esclava asociada 140, hay tres bloques correspondientes a los bloques mencionados anteriormente en la tarjeta maestra 130, concretamente un bloque receptor de configuraciones 410, un bloque receptor de programas 420 y un bloque receptor de comandos 430. En la tarjeta esclava 140, también hay un gestor de aplicaciones 400 que gestiona aplicaciones; en el aparato electrónico de oficina 150 asociado a la tarjeta 140, una o más aplicaciones 460 está/están adaptadas para interactuar con el gestor de aplicaciones 400.

[0084] Diversas aplicaciones 460 en el aparato electrónico de oficina 150 puede aprovecharse de la diversa información del abonado transferida, por ejemplo un gestor de inicio de sesión puede usar, por ejemplo, la información de identidad del abonado transferida, un navegador de Internet puede usar, por ejemplo, la información sobre el crédito y/o los derechos de abonado transferida, el sistema operativo puede usar, por ejemplo, la información de las preferencias del abonado transferida (idioma del abonado, ajustes de pantalla y de video, etc.).

[0085] Las aplicaciones 460 en el aparato electrónico de oficina 150 puede añadirse y/o mejorarse a través del procedimiento de programación que es implementado en la realización de la figura 2 esencialmente a través de los bloques 320 y 420. Esto puede aplicarse también a aplicaciones almacenadas en la tarjeta esclava 140.

[0086] El procedimiento de programación puede implicar una transferencia/almacenamiento temporal o permanente de una aplicación. El primer caso es útil, por ejemplo, para mejorar aplicaciones (en la tarjeta esclava y/o en el aparato electrónico de oficina) y el segundo caso es útil para aumentar temporalmente el número y/o las funcionalidades de las aplicaciones a ejecutar en el aparato electrónico de oficina en relación con la proximidad de una tarjeta maestra. Debe observarse que la información necesaria para la mejora puede ser recibida por la tarjeta maestra desde el exterior, por ejemplo la red de telecomunicaciones 110.

[0087] El procedimiento de comando puede usarse, en principio, mediante cualquier aplicación, en la tarjeta maestra 130 (es decir aplicaciones 340) o en el terminal de telefonía móvil 120 (es decir aplicaciones 360 y 370). Esta funcionalidad es útil cuando una aplicación en el terminal de telefonía móvil 120, en particular en la tarjeta maestra asociada 130, tiene la necesidad de comunicarse/interactuar con una aplicación en el aparato electrónico de oficina 150, en particular en la tarjeta esclava asociada 140; éste es típicamente el caso del control remoto de una aplicación.

[0088] Tal como ya se ha dicho, el canal de comunicación entre el bloque 330 y el bloque 430 es bidireccional, dado que a cada comando puede seguirle una respuesta, por ejemplo confirmación de que el comando

ha sido recibido o ejecutado correctamente.

[0089] Pueden proporcionarse comandos específicos que permiten descargar nuevas aplicaciones (por ejemplo aplicaciones 340 y/o 350 y/o 360 y/o 370) desde la tarjeta esclava 140 a la tarjeta maestra 130; en este caso, el flujo de datos desde la tarjeta esclava 140 a la tarjeta maestra 130 no está constituido por simples respuestas. En general, pueden transferirse aplicaciones (y seguidamente almacenarse) desde el aparato electrónico de oficina, y/o desde la tarjeta esclava asociada, al terminal de telefonía y/o a la tarjeta maestra asociada, pasando a través de una o más tarjetas inteligentes.

10 **[0090]** Las comunicaciones entre la tarjeta maestra 130 y la tarjeta esclava 140, es decir el canal de comunicación 30, pueden ser de tipo encriptado. En el caso en el que se usa la tecnología ZigBee™, el encriptado es a nivel físico; en general, siempre existe la posibilidad de implementar un canal seguro entre las dos tarjetas a nivel de la aplicación usando tecnologías conocidas.

15 **[0091]** Merece la pena observar que el término “maestra” no se refiere necesariamente a la entidad que inicia la comunicación con la “esclava”; la tarjeta esclava puede comenzar con un mensaje que solicita información a la tarjeta maestra y la tarjeta maestra puede responder transfiriendo la información solicitada. Por ejemplo, un gestor de inicio de sesión en ejecución en el aparato electrónico de oficina asociado con una tarjeta esclava puede emitir una solicitud del par nombre del usuario/contraseña; si la tarjeta esclava ya ha recibido estas credenciales de una tarjeta maestra, el gestor de inicio de sesión los usará para iniciar la sesión, en caso contrario el gestor de inicio de sesión enviará un mensaje de solicitud a cualquier terminal de telefonía móvil (asociado a una tarjeta maestra) ubicado en sus proximidades por medio de la tarjeta esclava y esperará una respuesta.

25 **[0092]** Una implementación del diálogo entre la tarjeta maestra 130 y la tarjeta esclava 140 en caso de control remoto de una aplicación puede ser, por ejemplo, la siguiente:

1) La tarjeta maestra 130 envía un comando de “conexión” a la tarjeta esclava 140 usando el bloque 330 para construir el canal de comunicación;

30 2) La tarjeta esclava 140 envía una respuesta de “conexión con éxito” para confirmar la recepción del comando usando el bloque 430;

3) La tarjeta maestra 130 envía un comando de “solicitud de aplicación a control remoto” para realizar la búsqueda de una aplicación específica en la tarjeta esclava 140 usando el bloque 330;

35 4) La tarjeta esclava 140 envía una respuesta de “aplicación disponible” para confirmar la recepción del comando usando el bloque 430;

40 5) La tarjeta maestra 130 envía comandos remotos a la tarjeta esclava 140 (específicamente a la aplicación a controlar) usando el bloque 330;

6) La tarjeta esclava 140 envía respuestas de confirmación para cada comando ejecutado usando el bloque 430;

45 7) al terminar la aplicación, la tarjeta maestra 130 envía un comando de “desconexión” a la tarjeta esclava 140 usando el bloque 330 para liberar la aplicación; y

8) la tarjeta esclava 140 envía una respuesta de “desconexión con éxito” para confirmar la recepción del comando usando el bloque 430.

50 **[0093]** Tal como se muestra en la figura 3, desde el punto de vista del software, la tarjeta maestra 130 y la tarjeta esclava 140 pueden dividirse en dos partes. La primera es la capa de software de radio de proximidad 130B y 140B y la segunda es la capa de software de la aplicación 130A y 140A. Las dos capas están conectadas mediante un canal de comunicación interno 60 y 70, que puede ser físico o lógico según la implementación de las tarjetas. Ventajosamente, la presente invención permite separar la capa de la aplicación de la capa de radio, de modo que el desarrollo del software pueda ser independiente.

[0094] La separación puede obtenerse definiendo una interfaz común entre la capa de la aplicación y la capa de radio de la siguiente manera:

- “Activar”: activar la comunicación de la capa de radio
- “Enviar”: enviar un comando/respuesta a otra tarjeta, a través del canal de radio de proximidad
- 5 • “Recibir”: recibir una respuesta/comando de otra tarjeta, a través del canal de proximidad
- “Controlar”: enviar un comando de control/configuración a la capa de radio

- “Desactivar”: desactivar la capa de radio

10

[0095] Las funciones anteriores permiten construir la arquitectura de firmware descrita anteriormente y transportar comandos específicos.

15 **[0096]** Desde el punto de vista de la capa de radio, hay dos tipos de comandos procedentes de la capa de la aplicación: “a pasar” (PAS) y “a analizar” (PAR).

[0097] En referencia a la figura 3, los comandos PAS son transmitidos directamente a otra tarjeta por la capa de radio 130B sin ser analizados; los comandos PAR son analizados y ejecutados en la capa de radio 130B.

20 **[0098]** Los conceptos de PAR y PAS también pueden aplicarse a funciones, es decir un grupo de comandos. Solamente se permiten las siguientes combinaciones:

- Función PAS que transporta comandos PAR;

25 • Función PAS que transporta comandos PAS;

- Función PAR que transporta comandos PAR;

[0099] A las funciones PAR no se les permite transportar comandos PAS.

30

[0100] La de “activar” es una función PAR y transporta un comando PAR para la capa de radio 130B. El comando es analizado y ejecutado realmente en la capa de radio 130B, que se prepara para realizar las operaciones de radio.

35 **[0101]** La de “enviar” es una función PAS. Es capaz de transportar comandos tanto PAR como PAS. En el primer caso (PAR), el comando transportado es enviado desde la capa de la aplicación 130A a la capa de radio 140B. A continuación el comando es analizado y ejecutado en la capa de radio. Esto es útil para la configuración remota de la capa de radio, por ejemplo para ajustar la potencia de radio de la tarjeta esclava 140 desde la capa de la aplicación de la tarjeta maestra 130. En el segundo caso (PAS), el comando transportado es enviado desde la
40 capa de la aplicación 130A a la capa de la aplicación 140A. El comando es analizado y ejecutado desde la capa de la aplicación, por ejemplo para mostrar la siguiente foto en la presentación del portátil.

[0102] La de “recibir” es una función PAS y transporta un comando PAS. Ésta es una función de devolución de llamada generada, por ejemplo, en la capa de la aplicación de la tarjeta esclava 140 después de una función de
45 “Enviar” de tarjeta maestra con comando PAS.

[0103] Debe observarse que las funciones de “Enviar” y “Recibir” pueden activarse con limitación de distancia. Por ejemplo, el estándar ZigBee™ permite definir el alcance de la transmisión de proximidad, de modo que es posible crear/habilitar servicios de proximidad según la distancia entre la tarjeta maestra y la tarjeta esclava. Esta
50 capacidad es útil para escenarios como inicio de sesión, pagos a través del móvil, etc.

[0104] La de “Control” es una función PAR y transporta comandos PAR. Esto se usa desde la capa de la aplicación 130A para fijar u obtener parámetros de radio relacionados con la capa de radio 130B.

55 **[0105]** La de “Desactivar” es una función PAR y transporta un comando PAR para la capa de radio 130B. El comando es analizado y ejecutado en realidad en la capa de radio 130B, que se apaga.

[0106] Las funciones de “Activar” y “Desactivar” son útiles para minimizar el consumo de energía. En el caso de tecnología ZigBee™, por ejemplo, estas funciones se usan de manera sincronizada de modo que la tarjeta

esclava es capaz de recibir comandos desde la tarjeta maestra justamente cuando son enviados los comandos. La tarjeta maestra y la tarjeta esclava activan la parte de radio justamente en un intervalo de tiempo particular, según se configuró al comienzo cuando se inicializa el canal de comunicación.

5 **[0107]** Las funciones anteriores pueden usarse para implementar todos los escenarios descritos anteriormente. En el control remoto de aplicaciones, por ejemplo, podrían implementarse las siguientes operaciones:

- “Activar”: realizar la operación de conexión.

10 • “Controlar”: comprobar la disponibilidad de aplicación a control remoto,

- “Enviar”: enviar comandos remotos (por ejemplo “siguiente foto”, “foto anterior”, “ir a la foto”, etc.),

- “Desactivar”: desconectar la aplicación a control remoto.

15

[0108] Debe observarse que, para simplificar la descripción de la interfaz común, las funciones anteriores se han descrito considerando la tarjeta maestra, es decir la tarjeta inteligente asociada al terminal de telefonía móvil y al abonado, como iniciadora de la comunicación; pero esto no debe interpretarse como una limitación de la presente invención.

20

[0109] Aunque la presente invención se centra en la enseñanza de un método, un aspecto importante se refiere a tarjetas inteligentes, específicamente una tarjeta maestra o tarjeta del abonado y una tarjeta esclava o tarjeta del aparato. A continuación se describirán sus características técnicas principales.

25 **[0110]** En general, según la presente invención, la tarjeta maestra (por ejemplo 130) es una tarjeta inteligente para uso en comunicaciones adaptada para asociarse a un aparato electrónico local (por ejemplo 120), en particular un terminal de telefonía móvil; almacena al menos información de identificación del abonado y comprende un bloque de configuración (por ejemplo 310) adaptado para transmitir la información de identificación del abonado almacenada a un aparato electrónico remoto (por ejemplo 150), en particular a una tarjeta inteligente (por ejemplo 30 140) asociada al aparato electrónico remoto; la información transmitida está adaptada y es suficiente para ser usada por el aparato electrónico remoto para proporcionar de forma autónoma un servicio.

[0111] Tal como ya se ha mencionado, en algunas aplicaciones, para usar un servicio, es necesario no solamente identificar al abonado sino también autenticarle; por lo tanto, puede ser necesario transferir también 35 información de autenticación del abonado. Éste es el caso de aplicaciones de comunicación tales como, por ejemplo, servicio de telefonía GSM. El bloque de configuración (por ejemplo 310) puede estar adaptado para transmitir no solamente información de identificación del abonado sino también información de los derechos del abonado y/o información del crédito del abonado y/o información de las preferencias del abonado al aparato electrónico remoto, en particular a la tarjeta inteligente asociada al aparato electrónico remoto.

40

[0112] La tarjeta maestra (por ejemplo 130) puede comprender también un bloque de programación (por ejemplo 320) adaptado para transmitir aplicaciones al aparato electrónico remoto, en particular a la tarjeta inteligente asociada al aparato electrónico remoto.

45 **[0113]** La tarjeta maestra (por ejemplo 130) puede comprender también un bloque de control (por ejemplo 330) adaptado para transmitir comandos de aplicación al aparato electrónico remoto, en particular a la tarjeta inteligente asociada al aparato electrónico remoto.

[0114] La tarjeta maestra (por ejemplo 130) puede comprender también una unidad de comunicación por 50 radio para comunicarse con aparatos electrónicos remotos, en particular con las tarjetas inteligentes asociadas a aparatos electrónicos remotos, en particular a través de tecnología ZigBee™.

[0115] La tarjeta maestra (por ejemplo 130) puede comprender también un detector de proximidad de radio asociado a un espacio de cobertura de radio y adaptado para detectar un aparato electrónico remoto, en particular 55 una tarjeta inteligente asociada a un aparato electrónico remoto, cuando está dentro de este espacio de cobertura de radio.

[0116] La tarjeta maestra según la presente invención puede comprender otras características; por ejemplo y típicamente, como la tarjeta 130, comprende al menos las características esenciales de una SIM o USIM telefónica.

[0117] En general, según la presente invención, la tarjeta esclava (por ejemplo 140) es una tarjeta inteligente para uso en comunicaciones, adaptada para asociarse a un aparato electrónico local (por ejemplo 150), en particular un aparato electrónico de oficina, para proporcionar un servicio; comprende un bloque de configuración (por ejemplo 5 410) adaptado para recibir y almacenar una información de identificación del abonado desde el aparato electrónico remoto (por ejemplo 120), en particular desde la tarjeta inteligente (por ejemplo 130) asociada al aparato electrónico remoto, y está adaptada para usar la información recibida para proporcionar de forma autónoma dicho servicio.

[0118] Tal como ya se ha mencionado, en algunas aplicaciones, para usar un servicio, es necesario no solamente identificar al abonado sino también autenticarle; por lo tanto, puede ser necesario recibir también información de autenticación del abonado. Éste es el caso de aplicaciones de comunicación tales como, por ejemplo, servicio de telefonía GSM.

[0119] El bloque de configuración (por ejemplo 410) puede estar adaptado para recibir también información de los derechos del abonado y/o información del crédito del abonado y/o información de las preferencias del abonado del aparato electrónico remoto, en particular desde la tarjeta inteligente asociada al aparato electrónico remoto.

[0120] La tarjeta esclava (por ejemplo 140) puede comprender también un bloque de programación (por ejemplo 420) adaptado para recibir aplicaciones del aparato electrónico remoto, en particular desde la tarjeta inteligente asociada al aparato electrónico remoto.

[0121] La tarjeta esclava (por ejemplo 140) puede comprender también un bloque de control (por ejemplo 430) adaptado para recibir comandos de aplicación del aparato electrónico remoto, en particular desde la tarjeta inteligente asociada al aparato electrónico remoto.

[0122] La tarjeta esclava (por ejemplo 140) puede estar adaptada, además, para transferir las aplicaciones recibidas y/o dichos comandos recibidos al aparato electrónico local asociado (por ejemplo 150).

[0123] La tarjeta esclava (por ejemplo 140) puede comprender también una unidad de comunicación por radio para comunicar con aparatos electrónicos remotos, en particular con tarjetas inteligentes asociadas a aparatos electrónicos remotos, en particular a través de tecnología ZigBee™.

[0124] La tarjeta esclava (por ejemplo 140) puede comprender un detector de proximidad de radio asociado a un espacio de cobertura de radio y adaptado para detectar un aparato electrónico remoto, en particular una tarjeta inteligente asociada a dicho aparato electrónico remoto, cuando está dentro de este espacio de cobertura de radio.

[0125] La tarjeta esclava según la presente invención puede comprender otras características; por ejemplo, como la tarjeta 140, comprende al menos las características esenciales de una SIM o USIM telefónica, tales como funcionalidades de autenticación del operador de red.

[0126] Debe entenderse que, una vez que la información de identidad del abonado y posiblemente la información de autenticación del abonado es transferida desde la tarjeta maestra a la tarjeta esclava, la tarjeta esclava tiene la información mínima necesaria para permitir que el aparato electrónico asociado proporcione de forma autónoma el servicio deseado, por ejemplo permitiendo llamadas telefónicas GSM de manera ordinaria, sin ayuda adicional de la tarjeta maestra.

[0127] Tal como ya se ha dicho, una tarjeta inteligente según la presente invención puede actuar como y, por lo tanto, tener las características tanto de una tarjeta maestra como de una tarjeta esclava.

[0128] En este caso, la tarjeta inteligente puede tener al menos dos modos de funcionamiento; en el primero usa la información del abonado almacenada previamente a nivel local y en el segundo usa información del abonado recibida a distancia; esto se aplica en particular a la información de identificación del abonado y posiblemente a la información de autenticación del abonado.

REIVINDICACIONES

1. Método de provisión de servicios que comprende las etapas de:
 - 5 A) proporcionar un aparato electrónico (150) asociado a una tarjeta del aparato (140), insertada en dicho aparato electrónico, y capaz de proporcionar un servicio por medio de información de identificación,
 - B) proporcionar un terminal de telefonía móvil (120),
 - 10 C) proporcionar una tarjeta del abonado (130) que almacena información de identificación del abonado, insertada en dicho terminal de telefonía móvil,
caracterizado porque comprende además:
 - D) transferir al menos dicha información de identificación del abonado desde dicha tarjeta del abonado (130) a dicha
15 tarjeta del aparato (140) cuando dicho terminal de telefonía móvil está en las proximidades de dicho aparato electrónico,
 - E) almacenar dicha información de identificación del abonado transferida en dicha tarjeta del aparato (140), y
 - 20 F) proporcionar dicho servicio por medio de dicha información de identificación del abonado transferida.
2. Método según la reivindicación 1, en el que dicho servicio es un servicio de comunicación proporcionado por dicho aparato electrónico.
- 25 3. Método según la reivindicación 1 o 2, que comprende además la etapa de:
 - G) proporcionar a dicho aparato electrónico (150) un detector de proximidad de radio asociado a un espacio de cobertura de radio y adaptado para detectar un terminal de telefonía móvil (120) cuando está dentro de dicho espacio de cobertura de radio.
- 30 4. Método según la reivindicación 1 o 2, en el que dicha tarjeta del abonado (130) y dicha tarjeta del aparato (140) comprenden, cada una, una unidad de comunicación por radio para comunicarse conjuntamente.
5. Método según la reivindicación 3, que comprende además la etapa de:
 - 35 H) eliminar o inhabilitar dicha información de identificación del abonado transferida cuando dicho terminal de telefonía móvil está fuera de las proximidades de dicho aparato electrónico.
6. Método según la reivindicación 1 o 2, en el que dicha etapa D permite transferir también información
40 de autenticación del abonado.
7. Método según la reivindicación 1 o 2, que comprende además la etapa de:
 - N) transferir aplicaciones desde dicho aparato electrónico (150) a dicho terminal de telefonía móvil (120), y
45 O) almacenar dichas aplicaciones transferidas en dicho terminal de telefonía móvil (120).
8. Método según la reivindicación 7, en el que dichas aplicaciones transferidas se almacenan en dicha tarjeta del abonado asociada (130) o pasan a través de dicha tarjeta del abonado asociada.
- 50 9. Tarjeta inteligente (130) para uso en comunicaciones, adaptada para insertarla en un terminal de telefonía móvil (120), que almacena información de identificación del abonado y que comprende un bloque de configuración adaptado para transmitir dicha información de identificación del abonado almacenada a una tarjeta inteligente (140) insertada en un aparato electrónico remoto (150), estando dicha información de identificación del
55 abonado transmitida adaptada y siendo suficiente para ser usada por dicho aparato electrónico remoto para proporcionar un servicio según el método de cualquiera de las reivindicaciones 1 a 8.
10. Tarjeta inteligente según la reivindicación 9, en la que dicho bloque de configuración está adaptado para transmitir también información de autenticación del abonado y/o información de los derechos del abonado y/o

información del crédito del abonado y/o información de las preferencias del abonado a dicha tarjeta inteligente (140) de dicho aparato electrónico remoto (150).

11. Tarjeta inteligente según la reivindicación 9, que comprende un bloque de programación adaptado para transmitir aplicaciones a dicha tarjeta inteligente (140) de dicho aparato electrónico remoto (150).

12. Tarjeta inteligente (140) para uso en comunicaciones, adaptada para insertarla en un aparato electrónico local (150) para proporcionar un servicio, que comprende un bloque de configuración adaptado para recibir y almacenar información de identificación del abonado desde una tarjeta inteligente (130) insertada en un terminal de telefonía móvil (120), y que está adaptada para usar dicha información de identificación del abonado recibida para proporcionar dicho servicio según el método de cualquiera de las reivindicaciones 1 a 8.

13. Tarjeta inteligente según la reivindicación 12, en la que dicho bloque de configuración está adaptado para recibir también información de autenticación del abonado y/o información de los derechos del abonado y/o información del crédito del abonado y/o información de las preferencias del abonado desde dicha tarjeta inteligente de dicho aparato electrónico remoto.

14. Tarjeta inteligente según la reivindicación 12, que comprende un bloque de programación adaptado para recibir aplicaciones desde dicha tarjeta inteligente (130) de dicho terminal de telefonía móvil (120).

15. Tarjeta inteligente que tiene las características de una o más de las reivindicaciones 9 a 11 y que tiene las características de una o más de las reivindicaciones 12 a 14, que tiene al menos dos modos de funcionamiento, en un primer modo de funcionamiento que usa información de identificación del abonado almacenada previamente a nivel local y en un segundo modo de funcionamiento que usa información de identificación del abonado recibida a distancia.

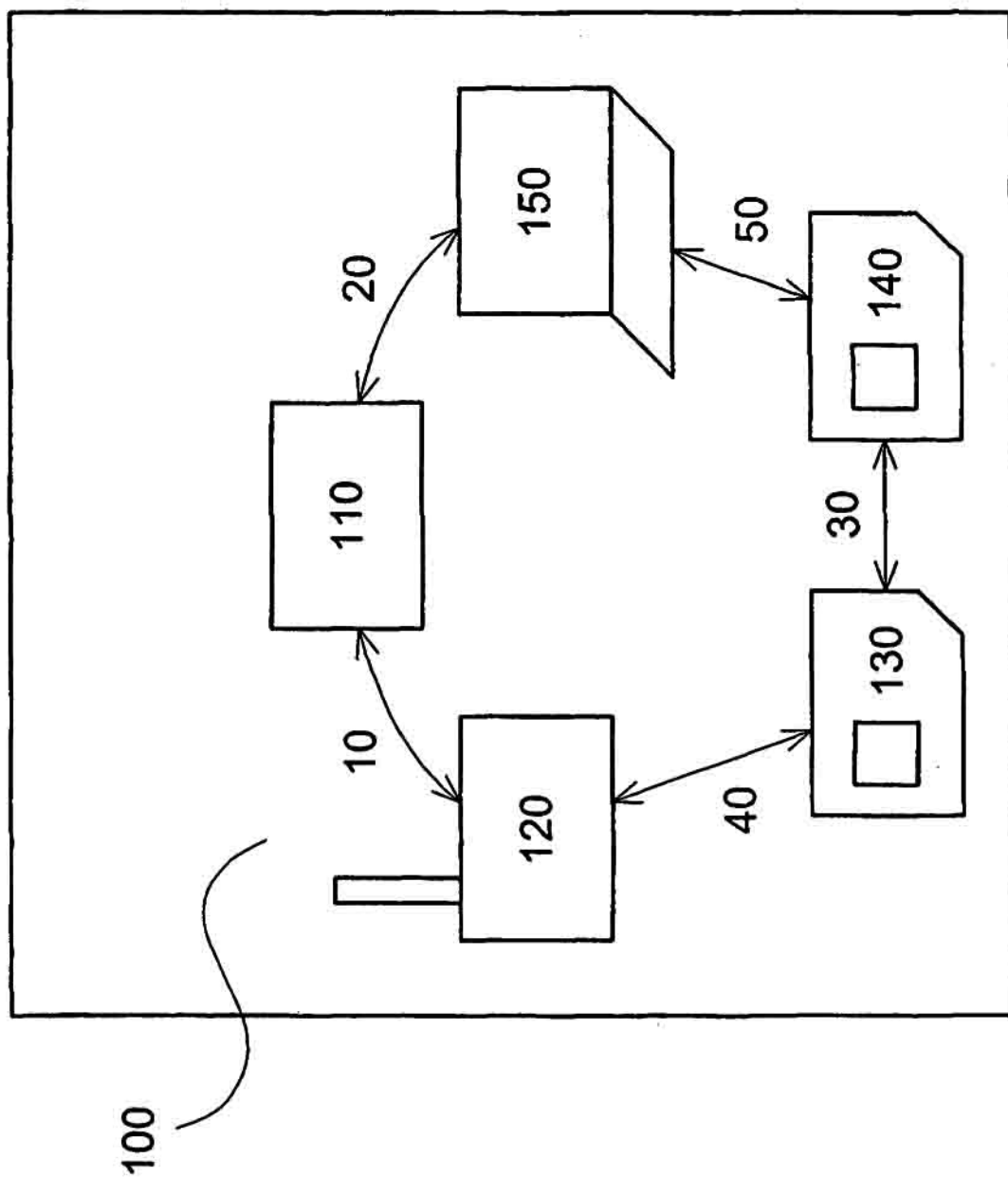


Fig.1

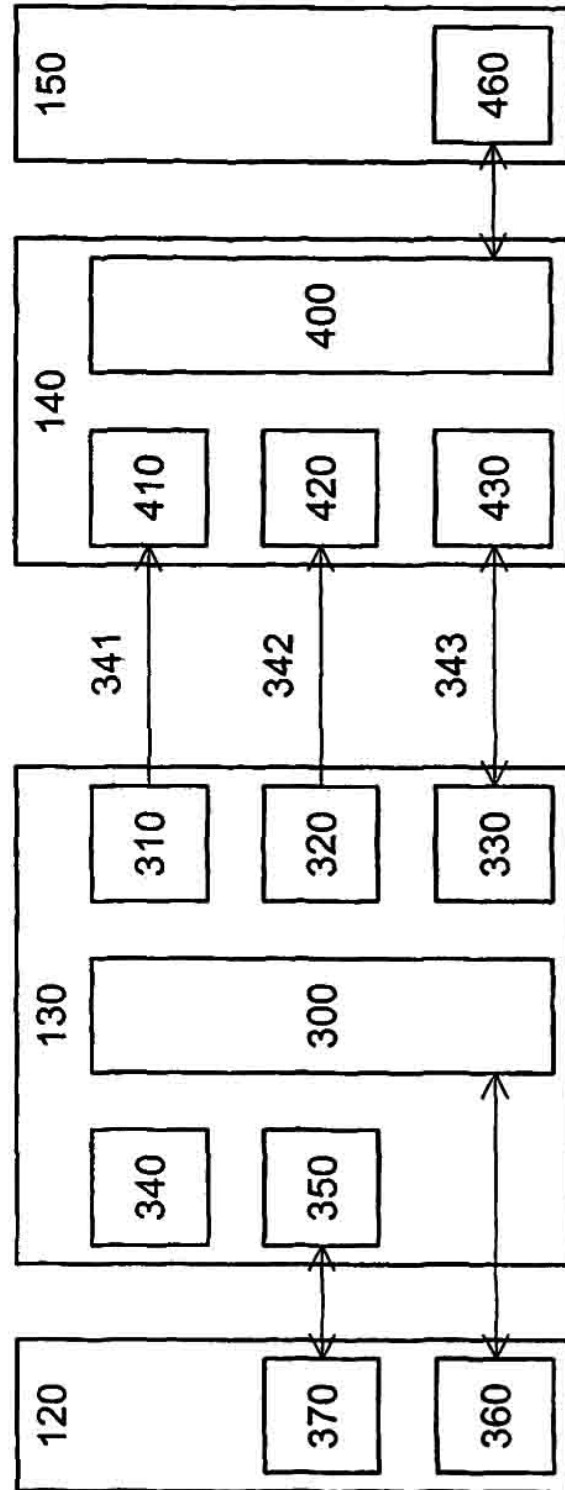


Fig.2

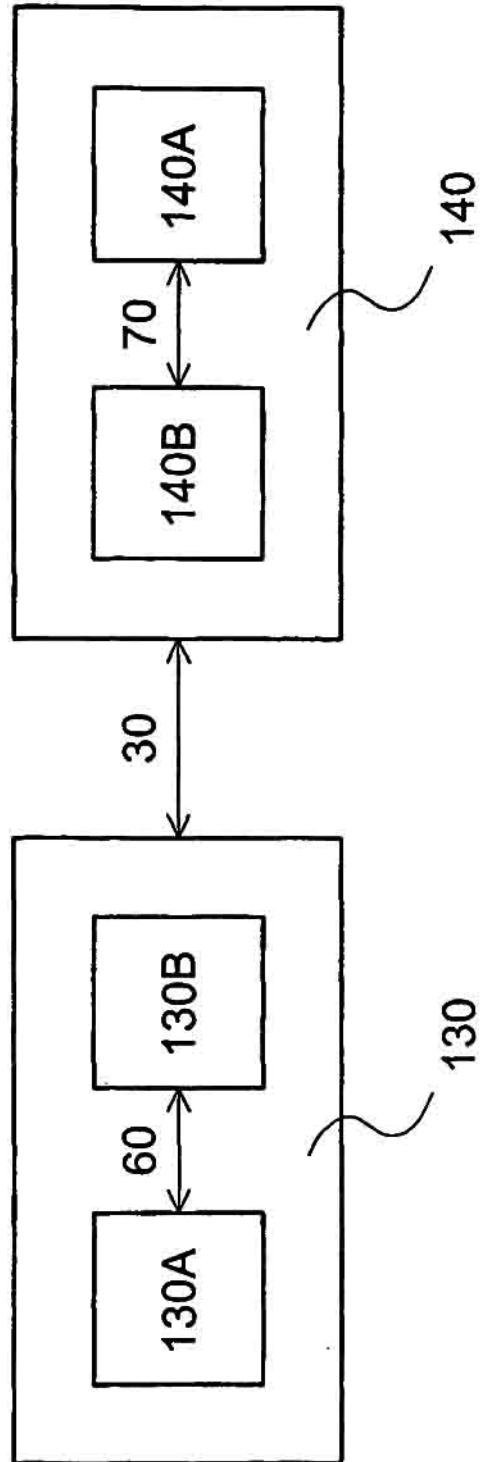


Fig.3