(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 April 2013 (04.04.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/045924 A1

(51) International Patent Classification:
H04W 12/04 (2009.01) *H04L 29/06* (2006.01)
H04W 12/06 (2009.01) *H04L 29/00* (2006.01)

(21) International Application Number:
PCT/GB2012/052388

(22) International Filing Date:
26 September 2012 (26.09.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1116529.7 26 September 2011 (26.09.2011) GB

(71) Applicant *(for all designated States except US)*: **VALH)-SOFT UK LIMITED** [GB/GB]; 9 Devonshire Square, London, Greater London EC2M 4YF (GB).

(72) Inventors; and
(71) Applicants *(for US only)*: **PETERSEN, John** [AU/GB]; c/o ValidSoft UK Limited, 9 Devonshire Square, London Greater London EC2M 4YF (GB). **CARROLL, Pat** [IE/GB]; c/o ValidSoft UK Limited, 9 Devonshire Square, London, Greater London EC2M 4YF (GB). **ALFORD, Jon** [GB/GB]; c/o ValidSoft UK Limited, 9 Devonshire Square, London, Greater London EC2M 4YF (GB).

(74) Agent: **HARRISON GODDARD FOOTE;** 140 London Wall, London, Greater London EC2Y 5DN (GB).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: SECURE WIRELESS NETWORK CONNECTION METHOD

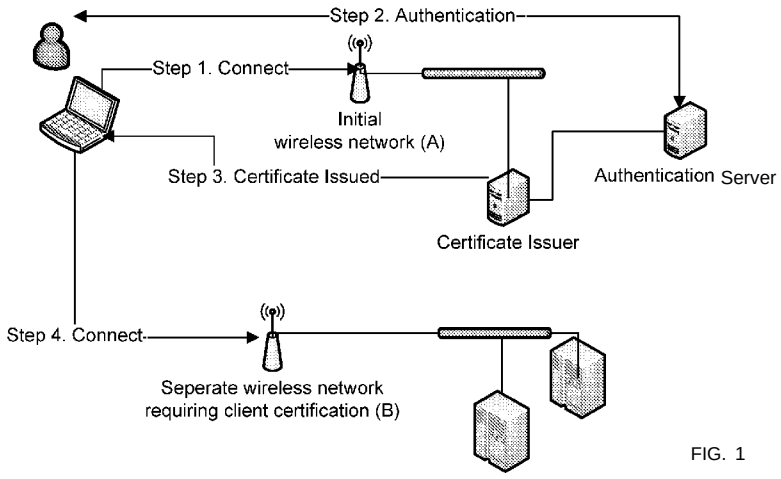

FIG. 1

(57) Abstract: A method of connecting a user computing device to a wireless network comprises establishing a wireless connection between the user computing device and a first wireless network. The user provides identifying information to a server via the first wireless network. In response to the server authenticating the user and upon successful authorisation of the user having the appropriate rights, the user receives access information for a second wireless network from the server. The user computing device establishes a wireless connection to the second wireless network using the received access information. The method has the advantage that the first wireless network can be easily discoverable, whereas the second wireless network can have an enhanced level of security.

WO 2013/045924 A1

SECURE WIRELESS NETWORK CONNECTION METHOD

[0001] This invention relates to a method of connecting a user computing device to a wireless network, as well as a user computing device, server, data communication system and computer software for implementing the method.

BACKGROUND

[0002] Wireless connectivity is a commonplace resource now in both residential, commercial and public sector/military environments. There has been a move from static systems with wired connections to laptops, tablets and handheld devices resulting in the availability and dependability of wireless network solutions becoming more important.

[0003] With a wireless network, there are risks that need to be reduced or, if possible, eliminated to ensure data integrity and security. Broadcasting data 'over the air' wirelessly introduces the risk that data is not directed just to the intended recipient, but to any recipient within range. So-called spoofing or impersonation of both sender and recipient introduces questions about whether the data transmitter- or receiver-party is a trusted party or not.

[0004] Authentication mechanisms serve as a means to identify peers connected to a network and encryption of data prior to transmission prevents eavesdropping and tampering. Using this system, a unique certificate is granted to devices upon having passed an initial verification process. The combination of these provides a very strong authentication, authorisation and accounting mechanism required for network access

BRIEF SUMMARY OF THE DISCLOSURE

[0005] In accordance with the present invention there is provided a method of connecting a user computing device to a wireless network. The method comprises establishing a wireless connection between the user computing device and a first wireless network. The user provides identifying information to a server via the first wireless network. In response to the server validating the identifying information provided by the user, the user receives access information for a second wireless network from the server. The user computing device establishes a wireless connection to the second wireless network using the received access information. Validation of the identifying information may comprise authenticating the user, i.e. confirming the user's identity, and determining the authorisation of the user to access the second wireless network.

[0006] Thus, in accordance with the invention, the user computing device can connect to a first wireless network that can have a relatively low level of security. Connection to the first wireless network can be relatively simple for the user or even automatic. The user can obtain access information for a second wireless network that can have a higher level of

security and/or encryption, or a user could be automatically joined to a second wireless network. In this way, the second wireless network does not need to be easily discoverable or accessible, which reduces the opportunities for unauthorised access to the second wireless network.

[0007] The user computing device may be, for example, a computer, a laptop computer, a tablet a personal digital assistant, a mobile telephone, a smartphone or any other suitable device capable of connecting to a wireless network. Typically, the user computing device will comprise a wireless network adapter. The wireless network adapter may be internal to the user computing device or may be external.

[0008] The first and/or second wireless networks may be a wireless local area network based on the IEEE 802.1 1 standard. However, other wireless network protocols may be used. It is not necessary for the first and the second wireless networks to operate using the same communications protocol.

[0009] The identifying information provided by the user computing device may be, for example, a username and password, an identifying code, or other similar identifier. The identifying information may be provided to the server via a secure connection, for example a secure socket layer (SSL) connection. The identifying information may be provided via a web application downloaded from the server by the user computing device. Alternatively, the user computing device may have software installed to provide the identifying information to the server.

[0010] As used herein, the term "server" is not limited to a single computer operating as a server and the term is used to include the possibility that the functionality of the "server" may be provided by a plurality of connected computers. For example, an access server may be provided to receive the identifying information from the user and a connected validation server may be provided to validate the identifying information.

[0011] Validation of the identifying information may require additional input from the user. For example, the user may be sent a validation code on a separate communication channel, for example via a mobile telephone, which must be provided to the server in order to complete the validation process.

[0012] In one embodiment of the invention, the user computing device receives the access information for the second wireless network from the server via the first wireless network. However, in embodiments of the invention the user is able to send and receive information, such as the access information, via a separate channel, for example via a mobile telephone. The advantage of the out of band factor is that, should a third party

have acquired access to, or duplicated, a user device or credentials, the authentication process requires additional steps increasing the security factor.

[0013] The server may notify a network access controller of the second wireless network that access information has been issued to the user. In this case, the network access controller may then expect an access request from the user, for example within a predetermined time period. The access information may include time-limited access credentials, which may be provided as an alternative or in addition to, for example, a MAC address, IP address, digital certificate and/or encryption key which could be configured to be prerequisite data for access to the second wireless network. The prerequisite data may be shared with the network access controller by the server in order that the network access controller is able to recognise the data and attributes when they are processed and facilitate access to the second wireless network.

[0014] Typically, the first wireless network broadcasts a network identifier. The network identifier may be a service set identifier (SSID). Broadcasting a network identifier simplifies identification of the network for the user. The second wireless network may not broadcast a network identifier. However, the access information may include the network identifier of the second wireless network. In this way, the user is able to identify and gain access to the second wireless network even though the network identifier is not broadcast.

[0015] The access information may include a password for access to the second wireless network. In an embodiment of the invention, the access information includes a digital certificate for secure access to the second wireless network. The digital certificate may include an encryption key. The digital certificate may be installed on the user computing device to allow secure access to the second wireless network.

[0016] Typically, the user computing device disconnects from the first wireless network before establishing the wireless connection to the second wireless network.

[0017] A particular advantage of the present invention is that the user has the convenience of connecting to the first wireless network while maintaining the higher level of security of the second wireless network. Consequently, the method is typically carried out while the user computing device is within the communication range of both the first and the second wireless networks. Thus, the communication range of the two wireless networks may be substantially the same or have a substantial overlap.

[0018] Viewed from a further aspect, the invention provides a user computing device configured to establish a wireless connection to a first wireless network, communicate identifying information from a user to a server via the first wireless network, in response to the server validating the identifying information provided by the user, receive access

information for a second wireless network from the server and establish a wireless connection to the second wireless network using the received access information.

[0019] The user computing device is typically configured to receive the access information for the second wireless network from the server via the first wireless network. The user computing device is typically configured to disconnect from the first wireless network before establishing the wireless connection to the second wireless network.

[0020] The invention also extends to computer software which configures a general-purpose computing device to operate as a user computing device in accordance with the invention. The computer software may take the form of an application that is installed on the user computing device and automatically carries out the steps of the invention. In this way, once the user has provided the identifying information, the user computing device may automatically receive the access information and connect to the second wireless network, disconnecting from the first wireless network as necessary.

[0021] Viewed from a yet further aspect, the invention provides a computer server configured to receive identifying information from a user computing device via a first wireless network, validate the identifying information provided by the user computing device, and in response to successful validation of the identifying information provided by the user computing device, communicate access information for a second wireless network to the user computing device. As explained above, the server may be provided by multiple interconnected computing devices.

[0022] The server may be configured to communicate the access information for the second wireless network to the user computing device via the first wireless network. The server may be configured to notify a network access controller of the second wireless network that access information has been issued to the user computing device.

[0023] The invention extends to computer software which configures a general-purpose computing device or a plurality of general-purpose computing devices to operate as a computer server according to the invention.

[0024] Viewed from a yet further aspect, the invention provides a data communication system comprising a first wireless device, an access server in data communication with the first wireless device and a second wireless device. The first wireless device is configured to establish data communication with a user computing device and to communicate identifying information from the user computing device to the access server. The access server is configured to validate the identifying information provided by the user computing device and, in response to successful validation of the identifying information, to communicate access information for a second wireless network to the user computing

device via the first wireless device. The second wireless device is configured to establish data communication with the user computing device on receipt of the access information.

[0025] The system may further comprise a network access controller in data communication with the second wireless device. The access server may be configured to notify the network access controller that access information has been issued to the user computing device. The network access controller may control the operation of the second wireless device.

[0026] The system may further comprise a logging system to record events on the first wireless network, the authentication process, the authorisation process and/or events on the second wireless network. This feature provides accounting and audit capability in respect of each component and user of the system.

[0027] The first wireless device may be configured to broadcast a network identifier. The second wireless device may be configured to operate without broadcasting a network identifier. The access information may include the network identifier of the second wireless device.

[0028] Typically, the first wireless device and the second wireless device are located such that a user computing device within the communication range of the first wireless device is also within the communication range of the second wireless device. For example, the first wireless device and the second wireless device may be located in substantially the same location. Indeed, the first wireless device and the second wireless device may be provided as a single physical unit.

[0029] The system may further comprise multiple secondary networks that users may be permitted to use. Upon successful authentication of a user, authorisation is determined based on rights/permissions attributed to that user and that are accessible by a server. A user can then be granted access information to a second network based on an individual basis or on membership of a larger group such as department, company or clearance level. In an embodiment of the invention, a user from a sales department, via the first network, is provided access information for a secondary network. Additionally a user from a technical department, via the same first network, is provided access information to a different secondary network.

BRIEF DESCRIPTION OF THE DRAWINGS

[0030] Embodiments of the invention are further described hereinafter with reference to the accompanying drawings, in which:

Figure 1 is a schematic diagram illustrating the operation of an embodiment of the invention.

DETAILED DESCRIPTION

[0031] In broad terms, embodiments of the invention relate to a process in which a client device connects to a visible primary network which can provide a 'limited' set of services. The client device can authenticate itself on the primary network in order to obtain certificates to allow connection to a secondary network(s) running a security protocol that requires clients to present the obtained certificate. Thus, the method involves certificate acquisition on one wireless network and, based on that acquisition, allowing communication with and connection to another (private/secure) network based on permission associated with the certificate. In order to use a certificate dependent wireless network (network B), the client needs to present some certificate data in the negotiation process of joining. This requires the client to have previously obtained the certificate prior to attempting such a connection. According to an embodiment of the invention, a guest or lobby network (network A) is used for the clients to connect initially, for acquisition of certificates to be used with another desired network. The system attempts to validate a user or device intending to connect, obtain and present a certificate together with information where and how to utilise it (i.e. network B, C, D etc.). The client processes this information, attempts to connect to the network indicated and with the acquired certificate.

[0032] An embodiment of the invention is illustrated in Figure 1. As shown in Figure 1, in Step 1 a client computer (illustrated as a laptop computer) connects to a wireless network (network A), which is typically accessible to all clients without requiring passwords or certificates. The client computer then establishes a secure connection to a certificate issuer. Typically the certificate issuer is presented as a server to which the client computer can connect using a web browser or application. The certificate issuer may be a service running on a local, trusted, network resource or may be a certificate issuer which operates over the Internet or other remote network.

[0033] In Step 2, the client user can authenticate themselves to the certificate issuer using a variety of different methods, such as username, password, hardware signature, one time token, out of band verification, biometrics, or a combination of multiple factors to determine accuracy and increased security. The client user provides identifying information via the secure connection on the initial wireless network to the certificate issuer. The certificate issuer communicates with an authentication server to confirm the authenticity of the client user's identifying information and determine the authorisation permitted. This may require additional information from the client user.

[0034] Once the authentication server confirms that the user's credentials are authentic and the user's rights permit them access further, at Step 3, the certificate issuer creates or authorises a certificate and issues this to the client, to be transmitted securely, stored and

registered locally on the client computer. In addition to the certificate, information is also passed securely to the client computer identifying the intended network (network B in this example) to which the client computer should connect using this certificate. The certificate and the identifying information is processed utilising a service, application, plug-in or similar implementation on the client computing device.

[0035] Once the certificate and network information have been safely received and stored, at Step 4 the client computer disconnects from the initial network and attempts to begin negotiation with the second wireless network in order to connect. Typically this network operates without broadcasting its identity (for example, its SSID), on separate infrastructure or using equipment capable of running multiple, segmented wireless networks to communicate with either the certificate issuer network or the more secure internal network(s). The client computer is now in a position to call upon the certificate and utilise aspects of the data available over the second wireless network (B) when required. This certificate data may be solely sufficient for the security requirements or can be utilised with other factors such as passwords.

[0036] After successful negotiation, the client computer is now a member of this second network and can connect directly whilst in possession of a valid and current client-held certificate. Such a certificate may have a short lifespan in order to increase security.

In summary, a method of connecting a user computing device to a wireless network comprises establishing a wireless connection between the user computing device and a first wireless network. The user provides identifying information to a server via the first wireless network. In response to the server authenticating the user and upon successful authorisation of the user having the appropriate rights, the user receives access information for a second wireless network from the server. The user computing device establishes a wireless connection to the second wireless network using the received access information. The method has the advantage that the first wireless network can be easily discoverable, whereas the second wireless network can have an enhanced level of security.

[0037] Throughout the description and claims of this specification, the words "comprise" and "contain" and variations of them mean "including but not limited to", and they are not intended to (and do not) exclude other moieties, additives, components, integers or steps. Throughout the description and claims of this specification, the singular encompasses the plural unless the context otherwise requires. In particular, where the indefinite article is used, the specification is to be understood as contemplating plurality as well as singularity, unless the context requires otherwise.

[0038] Features, integers and characteristics described in conjunction with a particular aspect, embodiment or example of the invention are to be understood to be applicable to any other aspect, embodiment or example described herein unless incompatible therewith. All of the features disclosed in this specification (including any accompanying claims, abstract and drawings), and/or all of the steps of any method or process so disclosed, may be combined in any combination, except combinations where at least some of such features and/or steps are mutually exclusive. The invention is not restricted to the details of any foregoing embodiments. The invention extends to any novel one, or any novel combination, of the features disclosed in this specification (including any accompanying claims, abstract and drawings), or to any novel one, or any novel combination, of the steps of any method or process so disclosed.

CLAIMS

1. A method of connecting a user computing device to a wireless network, the method comprising:

establishing a wireless connection between the user computing device and a first wireless network;

the user providing identifying information to a server via the first wireless network;

in response to the server validating the identifying information provided by the user, the user receiving access information for a second wireless network from the server;

the user computing device establishing a wireless connection to the second wireless network using the received access information.

2. A method as claimed in claim 1, wherein the user computing device receives the access information for the second wireless network from the server via the first wireless network.

3. A method as claimed in any preceding claim, wherein the server notifies a network access controller of the second wireless network that access information has been issued to the user.

4. A method as claimed in any preceding claim, wherein the first wireless network broadcasts a network identifier.

5. A method as claimed in any preceding claim, wherein the second wireless network does not broadcast a network identifier and the access information includes the network identifier of the second wireless network.

6. A method as claimed in any preceding claim, wherein the access information includes a certificate for secure access to the second wireless network.

7. A method as claimed in any preceding claim, wherein the user computing device disconnects from the first wireless network before establishing the wireless connection to the second wireless network.

8. A method as claimed in any preceding claim, wherein the method is carried out while the user computing device is within the communication range of both the first and the second wireless networks.

9. A user computing device configured to:

establish a wireless connection to a first wireless network;

communicate identifying information from a user to a server via the first wireless network;

in response to the server validating the identifying information provided by the user, receive access information for a second wireless network from the server;

establish a wireless connection to the second wireless network using the received access information.

10. A device as claimed in claim 9, wherein the user computing device is configured to receive the access information for the second wireless network from the server via the first wireless network.

11. A device as claimed in claim 9 or 10, wherein the access information includes a certificate for secure access to the second wireless network.

12. A device as claimed in any of claims 9 to 11, wherein the user computing device is configured to disconnect from the first wireless network before establishing the wireless connection to the second wireless network.

13. Computer software which configures a general-purpose computing device to operate as a user computing device according to any of claim 9 to 12.

14. A computer server configured to:

receive identifying information from a user computing device via a first wireless network;

validate the identifying information provided by the user computing device;

in response to successful validation of the identifying information provided by the user computing device, communicate access information for a second wireless network to the user computing device.

15. A server as claimed in claim 14, wherein the server is configured to communicate the access information for the second wireless network to the user computing device via the first wireless network.

16. A server as claimed in claim 14 or 15, wherein the server is configured to notify a network access controller of the second wireless network that access information has been issued to the user computing device.

17. A server as claimed in any of claims 14 to 16, wherein the access information includes a network identifier of the second wireless network.

18. A server as claimed in any of claims 14 to 17, wherein the access information includes a certificate for secure access to the second wireless network.

19. Computer software which configures a general-purpose computing device or a plurality of general-purpose computing devices to operate as a computer server according to any of claims 14 to 18.

20. A data communication system comprising:

a first wireless device;

an access server in data communication with the first wireless device; and

a second wireless device,

wherein the first wireless device is configured to establish data communication with a user computing device and to communicate identifying information from the user computing device to the access server,

wherein the access server is configured to validate the identifying information provided by the user computing device and, in response to successful validation of the identifying information, to communicate access information for a second wireless network to the user computing device via the first wireless device, and

wherein the second wireless device is configured to establish data communication with the user computing device on receipt of the access information.

21. A system as claimed in claim 20, wherein the system further comprises a network access controller in data communication with the second wireless device and the access server is configured to notify the network access controller that access information has been issued to the user computing device.

22. A system as claimed in claim 20 or 21, wherein the first wireless device is configured to broadcast a network identifier.

23. A system as claimed in any of claims 20 to 22, wherein the second wireless device is configured to operate without broadcasting a network identifier and the access information includes the network identifier of the second wireless device.

24. A system as claimed in any of claims 20 to 23, wherein the access information includes a certificate for secure access to the second wireless device.

25. A system as claimed in any of claims 20 to 24, wherein the first wireless device and the second wireless device are located such that a user computing device within the communication range of the first wireless device is also within the communication range of the second wireless device.

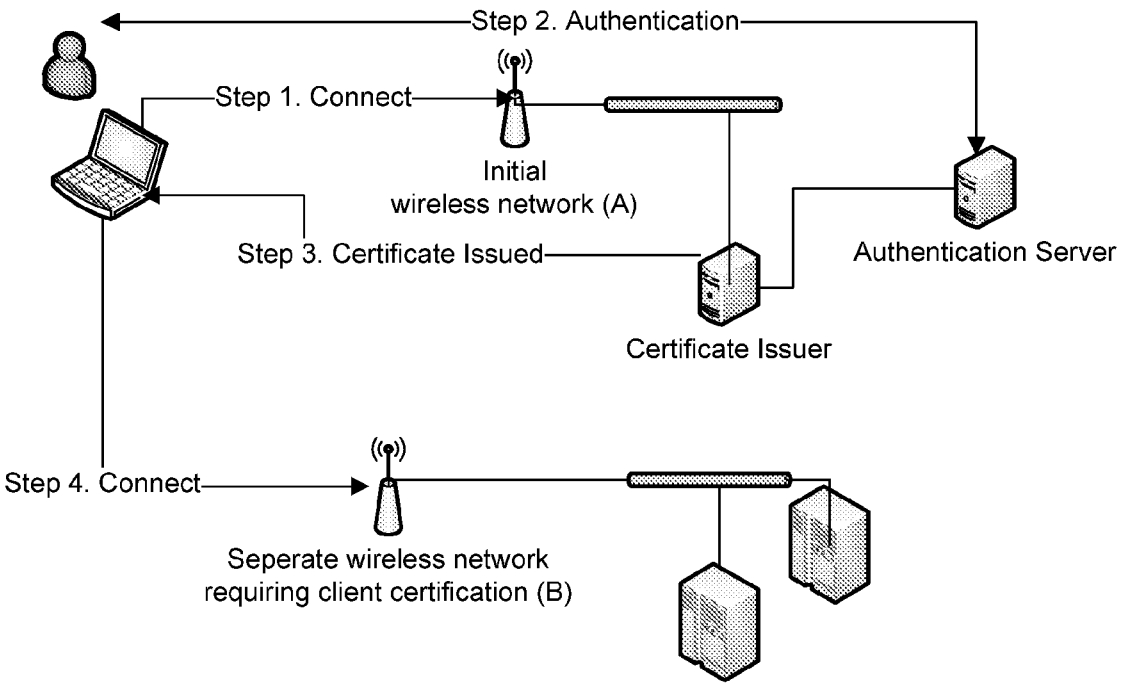
Step 2. Authentication
Step 1. Connect
Initial
wireless network (A)
Step 3. Certificate Issued
Authentication Server
Certificate Issuer
Step 4. Connect
Seperate wireless network
requiring client certification (B)

FIG. 1

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2012/052388

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/04 H04W12/06 H04L63/18 H04L63/08
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal , WPI Data, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2 096 829 Al (RESEARCH IN MOTION LTD [CA]) 2 September 2009 (2009-09-02) paragraphs [006Q] - [0072] , [0077] , [0080] figures 1-11	1-25
X	EP 2 348 763 A2 (FR DU RADIO TELEPHONE SFR S0C [FR]) 27 July 2011 (2011-07-27) paragraphs [0095] - [0118] paragraphs [0122] - [0140] figures 1-5	1-25
X	EP 2 199 944 A2 (CHARISMATHICS GMBH [DE]) 23 June 2010 (2010-06-23) paragraph [0020] paragraphs [0027] - [0029] , [0034] - [0038] figures 1-4	1-25

-/ -

X Further documents are listed in the continuation of Box C.

X See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) orwhich is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 November 2012	28/11/2012

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Ghomrasseni , Z

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2012/052388

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 928 125 A1 (RESEARCH IN MOTION LTD [CA]) 4 June 2008 (2008-06-04) paragraph [0003]	5,23

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/GB2012/052388

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2096829 Al	02-09-2009	AT 491298 T	15-12-2010
		CA 2655073 Al	29-08-2009
		EP 2096829 Al	02-09-2009
EP 2348763 A2	27-07-2011	EP 2348763 A2	27-07-2011
		FR 2955450 Al	22-07-2011
EP 2199944 A2	23-06-2010	DE 102008063864 Al	24-06-2010
		EP 2199944 A2	23-06-2010
EP 1928125 Al	04-06-2008	CA 2610112 Al	30-05-2008
		CN 101202686 A	18-06-2008
		EP 1928125 Al	04-06-2008
		JP 4642832 B2	02-03-2011
		JP 2008141755 A	19-06-2008
		KR 20080049678 A	04-06-2008