

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
21 June 2007 (21.06.2007)

PCT

(10) International Publication Number
WO 2007/068992 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/IB2005/003807

(22) International Filing Date:
16 December 2005 (16.12.2005)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **HAVERINEN, Henry** [FI/FI]; Einonkuja 10 A 3, FIN-40250 Jyväskylä (FI). **JAKKOLA, Mikko** [FI/FI]; Seurakuntaralontie 9, FIN-37560 Lempäälä (FI). **LOUGHNEY, John** [US/FI]; Aamutie 12 A 3, FIN-02210 Espoo (FI).

(74) Agent: **FALLER, Jürgen**; C/ o TBK-Patent Bavariaring 4-6, 80336 Munich (DE).

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

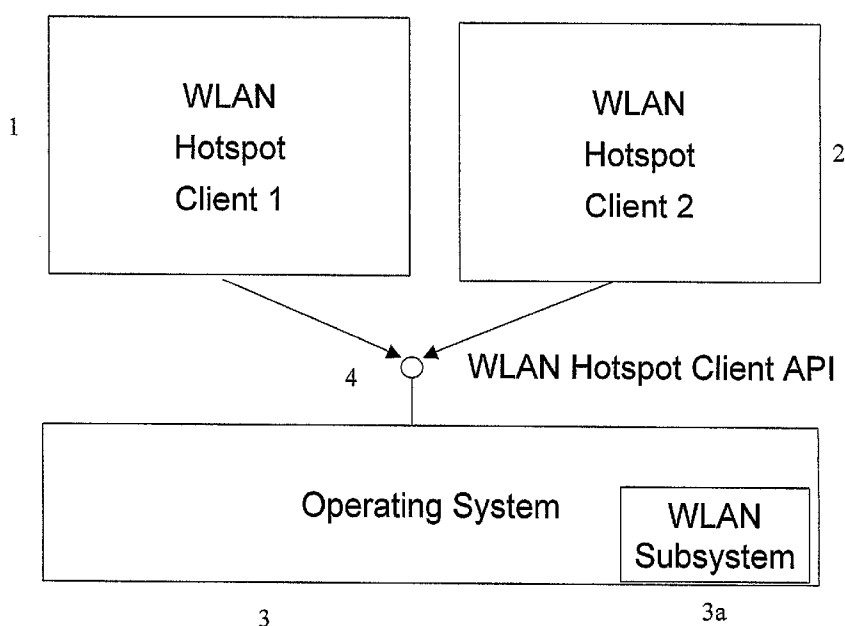
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SUPPORT FOR INTEGRATED WLAN HOTSPOT CLIENTS



(57) Abstract: The invention proposes a method and a network device comprising an operation entity (3) for handling network connection and at least one access client entity (1, 2) providing connection handling to a specific network access device, wherein the operation entity is adapted to identify a need for a network connection and to inform the access client entity, and the at least one access client entity is adapted to perform an authentication. Hence, an authentication procedure is delegated to a separate entity so that depending on the specification of a specific network connection, a suitable access entity for performing the authentication can be selected.

WO 2007/068992 A1

- 1 -

TITLE OF THE INVENTION: Support For Integrated WLAN
Hotspot Clients

BACKGROUND OF THE INVENTION:

5

Field of the invention

The invention relates to a method and a network device
for handling a network connection, wherein an access
10 client entity and an operation entity of the network
device can co-operate.

Description of the related art

15 The invention is in particular related to WLAN (Wireless
Local Area Network) Hotspot Clients, although it is not
limited thereon.

WLAN (Wi-Fi) has a large deployed base in enterprises,
20 homes and in hotspots. There has been a business model
developed around the use of public access Wi-Fi; with
service providers providing either time based charging or
subscription based charging. This industry is still in
its infancy, with many players competing for position.

25 There are a number of proprietary mechanisms deployed for
enabling provider authorization and authentication of
users within a hotspot.

Many hotspot operators are small, and in general the
30 operators have very heterogeneous equipment. The service
is very typically based on the "old" IEEE 802.11b
standard. Most hotspots do not support the new security
standards (IEEE 802.1x or WiFi Protected Access), or the
new physical layer standards such as the fast IEEE
35 802.11g or the 5 GHz IEEE 802.11a. Therefore, WLAN

- 2 -

aggregators (companies which provide brokering and aggregation for many different hotspot deployments) generally tend to concentrate on very simple equipment and HTTP-based (browser based) access control. In

5 practice, this means users need to start a web browser, and browse to a web page. The hotspot captures their traffic and redirects them to a centralized login page, where the user will need to present the proper credentials for gaining access in the hotspot.

10

Many WLAN aggregators and hotspot operators have developed proprietary automated logon clients, by which the user can discover the hotspot and log in easily, usually with one click. The hotspot clients are stand-
15 alone networking applications, and the authentication protocol is most often based on IP-layer protocols such as HTTP, TLS, XML, and not on IEEE standards.

The main logical functions of a Wi-Fi hotspot client are
20 summarized here.

Many hotspot clients include a directory tool that can be used off-line, for example before a business trip, to list hotspots per location, so that user can find out the
25 nearest compatible Wi-Fi hotspot. The information in the directory can be regularly updated, and it may include maps and images of the location.

The hotspot client usually includes a WLAN Sniffer, which
30 shows locally available WLAN networks. At least the network name (SSID (Service Set Identifier)) and the signal strength are displayed. Possibly, the sniffer can show richer information in addition to SSID, such as whether this is a "Sonera Homerun" network - or even hide
35 the technical SSID parameter from the user completely. In

- 3 -

the existing Windows and Pocket PC solutions, the WiFi sniffer tool can usually be used in manual network selection - to select the network to join. The user can also use the sniffer to manage SSID lists, network
5 priorities, or other connection settings of the provider for automatic network selection. There is usually a "Connect" button, by which the user can launch the automated log-on protocol. The WLAN sniffer, when combined with the directory tool enables users to quickly
10 know which hotspots they have access to, via their WLAN subscription.

The third feature of current WiFi clients is the actual logon client. It provides for easy authentication, so
15 that the user does not need to use the browser. Username, realm and password (or other credentials) are stored in the device. In cases when Network Access Identifier decoration is required, it is automatically applied. For compatibility with legacy 802.11b-only networks, the
20 logon protocol is typically an IP-based automated variant of web browser login.

Current hotspot clients are stand-alone applications, which the user must explicitly launch.

25

In the following, some more sophisticated approaches are described, in particular with respect to Symbian WLAN Networking and Seamless Roaming.

30 In Nokia's WLAN phones, WLAN settings can be included in Internet Access Point settings. The Internet Access Point setting can contain a SSID, or in the future, a list of SSIDs. The connection monitor, bearer manager and mobility policy manager components constantly try to
35 detect, which Internet Access Points are currently

- 4 -

available. It is also possible to learn, which SSIDs are available in the current neighborhood. For WLAN Internet Access Points, the availability is based on WLAN scanning and the SSID settings of each WLAN Internet Access Point.

5

Internet Access Points that provide connectivity to the same target network, such as the office intranet or the public Internet, can be grouped into a service network. The Internet Access Points can be given priorities, so that when opening a connection to a certain service network, the middleware can automatically select the most preferred available Internet Access Point. In the Nokia platform, when creating a connection, the application may use the RConnection API (Application Programming Interface) to open the connection to a certain service network. Once the connection has been successfully established, the application can start using it.

When the user wants to perform a task, such as send an e-mail message, with a Nokia mobile device, the user can usually directly launch the appropriate application, such as the e-mail client. When the e-mail client needs a connection to the Internet, the system will establish the connection. The e-mail client may be pre-configured with the correct connection information, or the user may be prompted to select the connection among a list of available connections. Even when a Virtual Private Network (VPN) connection to a private network is required, the system will automatically establish the VPN connection. Hence, the user does not need to switch on any radios or VPN clients before launching the e-mail application.

A problem with the present WLAN hotspot authentication mechanisms is that the user is required to use the WLAN

- 5 -

connection from a separate application (either the browser or stand-alone hotspot client) in order to be allowed to use the hotspot service, before using the e-mail application in the above-mentioned example.

5

There is a user need for automated roaming between Internet Access Points; which is also supported in the Nokia platform. In automated roaming, the application can receive a notification when a more preferred Internet
10 Access Point within the application's current service network has become available. The application can then close its current connection and reconnect using the newly discovered Internet Access Point. In network-level roaming, a middleware component, such as a VPN client or
15 a mobile IP client manages mobility between underlying Internet Access Points, transparently to the applications.

Thus, summarizing, the "normal" way for user to gain WLAN
20 access via a hotspot is:

- Manual log-in

1. A user reads a sign, showing that there is a hotspot.
2. User open the browser and tries to browse to a well-
25 known web page.
3. The user is redirected to the hotspot provider's web page.
4. The user is required to enter a user name & password in order to be authenticated & allowed to access hotspot.

30

- Semi-automated mechanism

1. User has installed software that has pre-configured authentication mechanism.
2. User clicks on software which finds a hotspot.

- 6 -

3. The user selects a hotspot, which calls an authentication 'script'.
4. The script then authenticates the user to a backend server
- 5 5. The user can then use the hotspot freely.

That is, the user opens a browser when he is inside a hotspot. When the user attempts to browse to a webpage, the user is re-directed to a portal page. The user can
10 then enter a User Name / Password. Once authenticated, the user is able to use the WLAN network. This is in particular inconvenient for handheld devices (like smart phones) as it requires the user to be aware of the surrounding wireless networks and perform more steps in
15 order to be connected.

Alternately, some hotspot aggregators use scripts which signal a backend server, mimicking the web page based login described above. These scripts are not completely
20 automated, however, and require user action.

Thus, still some manual input from the user is required in order to connect and de-connect via a Hotspot. That is, the user of a mobile terminal having WLAN has to
25 first establish a link layer connection and thereafter start the hotspot client in order to be able to use the network connection, e.g., to use the Internet.

Additionally, wireless signals are affected by
30 environmental factors. Walls, for example, can reduce the signal strength of wireless radios. Other wireless networking technologies, such as Bluetooth, can cause interference with WLAN signals. Therefore, a user might loose or gain a wireless connection based upon
35 environmental issues. If a user loses a connection to the

- 7 -

WLAN hotspot because another user happens to use a Bluetooth-enabled device, then the WLAN user must perform the steps listed above to regain the connection to the WLAN hotspot.

5

SUMMARY OF THE INVENTION

Hence, it is an object of the present invention to solve the problem mentioned above and to provide support for an easy and automated logon to an access entity such as a WLAN hotspot.

This object is solved by a method for handling a network connection of a network device comprising an operation entity for handling network connection, wherein at least one access client entity providing connection handling to a specific network access device is connectable to the operation entity, the method comprising the steps of identifying, by the operation entity, a need for a network connection, requesting the access client entity to perform authentication, and performing, by the access client entity, the authentication.

25

Alternatively, the object is solved by a method for operating an operation entity for handling network connection, wherein at least one access client entity providing connection handling to a specific network access device is connectable to the operation entity, the method comprising the steps of identifying, by the operation entity, a need for a network connection, and requesting the access client entity to perform authentication.

35

- 8 -

As a further alternative, the above object is solved by a method for operating an access client entity for handling a network connection to a specific network access device, connectable to a network device comprising an operation entity for handling network connection, the method comprising the steps of

receiving a request from the operation entity to perform authentication, and
performing the authentication.

Moreover, the above object is solved by a network device comprising an operation entity for handling network connection and at least one access client entity providing connection handling to a specific network access device, wherein

the operation entity is adapted to identify a need for a network connection and to inform the access client entity, and
the at least one access client entity is adapted to perform an authentication.

Alternatively, the above object is solved by an access client entity providing connection handling for a specific network access device, comprising
means for receiving a request to perform authentication from an operation entity, and
means for performing the authentication.

Further alternatively, the above object is solved by an operation entity for handling network connection, the operation entity comprising
means for identifying a need for a network connection, and

- 9 -

means to request an access client entity providing connection handling for a specific network access device to perform an authentication.

5 Hence, according to the invention, the authentication procedure is delegated to a separate element, namely an access client entity (an example therefore being a hotspot client). This access client entity can be specific for a specific network access device, so that no
10 manual input from the user is required.

Thus, according to the invention, the authentication is integrated into the connection subsystem.

15 Hence, the authentication process is simplified allowing any application, such as email, to gain access to the hotspot without requiring additional steps by the user.

According to a further aspect of the invention, the
20 operation entity may be informed about the result of the authentication by the access client entity, and, in case the authentication was successful, the operation entity may allow use of the network connection.

25 According to another aspect of the invention, a plurality of access client entities may be provided, and an access client entity of the plurality of access client entities may be selected based on the need for a network connection.

30

According to another aspect of the invention, a message may be sent from the access client entity to the operating system client to request the operating system client to notify when a certain connection profile
35 becomes available. Alternatively, a message may be sent

- 10 -

from the operating system client to the access client entity to request the access client entity to notify when a certain connection profile becomes available.

- 5 According to another aspect of the invention, a message may be sent from the operation entity to the access entity client by which the operation entity requests the access client entity to perform the authentication.
- 10 According to a further aspect of the invention, a message may be sent from the operation entity to the access entity client by which the operation entity requests the access client entity to perform a de-authentication.
- 15 According to another aspect of the invention, a message may be sent from the access client entity to the operation entity by which the access client entity indicates to the operating system that the authentication has been successfully performed.
- 20 According to another aspect of the invention, a message may be sent from the access client entity to the operation entity by which the access client entity indicates to the operating system that de-authentication
- 25 has been successfully performed.

- According to a further aspect of the invention, a message may be sent from the access client entity to the operation entity by which the access client entity
- 30 indicates to the operating system that authentication/de-authentication has failed.

- According to another aspect of the invention, a modification of a network connection setting by a user
- 35 input is prohibited.

- 11 -

According to a further aspect of the invention, an access client entity is registered to the operation entity..

- 5 According to another aspect of the invention, an access client entity is linked to a profile, wherein in the authenticating step, the operation entity informs the access client entity linked to the profile in case a connection with the profile is to be established.

10

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is described by referring to the enclosed
15 drawings, in which:

Fig. 1 shows a block diagram of the architecture according to an embodiment of the present invention,

- 20 Fig. 2 shows a message sequence chart illustrating a registration of a hotspot client according to the embodiment of the present invention,

Fig. 3 shows a message sequence chart illustrating an
25 automatic hotspot login according to the embodiment of the present invention,

Fig. 4 shows a message sequence chart illustrating an
automatic hotspot logoff according to the embodiment of
30 the present invention,

Fig. 5 shows a message sequence chart illustrating a WLAN availability discovery and authentication according to the embodiment of the present invention, wherein the
35 hotspot client manages discovery settings,

- 12 -

Fig. 6 shows a message sequence chart illustrating an WLAN availability discovery and authentication according to the embodiment of the present invention, wherein the OS manages discovery settings,

Fig. 7 shows a message sequence chart illustrating an the basic middleware enabled hotspot authentication according to the embodiment of the present invention in more detail,

Fig. 8 shows a message sequence chart illustrating the WLAN availability discovery and authentication according to the embodiment of the present invention in more detail, and

Fig. 9 shows a message sequence chart illustrating the WLAN hotspot de-authentication according to the embodiment of the present invention in more detail.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

In the following, a preferred embodiment of the present invention is described by referring to the attached drawings.

As described above, currently WLAN hotspot clients are currently used for an automated hotspot logon. To allow the implementation of such clients to operating systems such as Symbian, and to integrate the automated WLAN hotspot logon with networking of such an operating system, according to the embodiment there is provided - a mechanism to delegate the management of WLAN selection (SSID) to a separate client, and

- 13 -

- a mechanism to integrate a WLAN hotspot client with seamless roaming and with native user interfaces.

In more detail, according to the present embodiment, the
5 following is provided:

A WLAN Internet Access Point setting that indicates that the SSID settings are managed by an external software entity. When a WLAN Internet Access Point setting has
10 been configured with such an indication, the operating system knows that it is not responsible for detecting the availability of the Internet Access Point. The operating system may also detect that the user should not be able to use the standard user interfaces to modify the WLAN
15 settings, because WLAN settings are managed by a separate software entity. An embodiment of this setting is a special value of the existing SSID field that indicates an undefined SSID.

20 Moreover, an Application Programming Interface (API) is defined between the operating system and a 3rd party hotspot client. The API enables the following features:

- Subsequent installation of a 3rd party hotspot client
25 or several clients
- Automatic activation of a 3rd party hotspot client (or a notification to the hotspot client) by the WLAN subsystem or the operating system when the WLAN subsystem or the operating system detects a need to log on to a
30 WLAN network discovered by the WLAN subsystem system
- Capability to deliver notifications of events from the hotspot client to the WLAN subsystem or the operating system. Notifications could be given in the following events: discovery of a suitable network by the hotspot
35 client, successful authentication, unsuccessful

- 14 -

authentication (with various reason codes), authenticated session terminated, successful log-out, unsuccessful log-out

- 5 - Capability to deliver notifications of events from the WLAN subsystem or the operating system to the hotspot client. Notifications could be given in the following events: need to log in, need to log out.

- 10 Implementing roaming decisions or automatic Internet Access Point selection by the operating system, based on notifications given by a 3rd party hotspot client. For example, the "link up" notification about a WLAN Internet Access Point should be given to an application only after the authentication has been successfully completed, or
15 mobile IP registration should be tried after successful authentication.

In the following, the principles of the embodiment are described by referring to Figs. 1 to 6.

20

- In Fig. 1, an overview of the software architecture is shown, which is provided in a network device such as a smart phone, laptop, PDA or the like. Reference numeral 1 denotes a WLAN hotspot client 1 as an example for a first
25 access client entity (access client device), and reference numeral 2 denotes a WLAN hotspot client 2 as an example for a second access client entity (access client device). Reference numeral 3 denotes an Operating System (OS) as an example for an operation entity (operation
30 device), and reference numeral 3a denotes a WLAN subsystem integrated in the operating system 3. Reference numeral 4 denotes a WLAN hotspot client API.

- 35 Preferably, the following features should be available in the API 4.

- 15 -

• The API should be able to register a 3rd party hotspot client (e.g., the WLAN hotspot client 1 and/or 2) to the authentication framework of the operating system. The
5 hotspot client might be implemented as a dynamic link library that exports a standard hotspot client interface. Upon the registration, the operating system learns the file name of the library, and the operating system will later be able to call various methods in the hotspot
10 client.

• The API 4 should be able to link a 3rd party hotspot client (e.g., the WLAN hotspot client 1 and/or 2) to a profile. This means that when a connection with the
15 profile is established, the operating system will call the linked hotspot client to perform authentication.

In addition, the following primitives should be defined for the API:

20

• An API primitive by which the hotspot client can request the operating system to notify when a certain connection profile becomes available (used when the operating system manages WLAN network discovery
25 settings).

• An API primitive by which the operating system can request the hotspot client to notify when a certain connection profile becomes available (used when the
30 hotspot client manages WLAN network discovery settings).

• An API primitive by which the operating system can request the hotspot client to perform authentication.

- 16 -

- An API primitive by which the operating system can request the hotspot client to perform de-authentication.
- An API primitive by which the hotspot client can
5 indicate to the operating system that authentication has been successfully performed.
- An API primitive by which the hotspot client can
10 indicate to the operating system that de-authentication has been successfully performed.
- An API primitive by which the hotspot client can
indicate to the operating system that authentication/de-authentication failed.

15

In the following, the operation of the operating system and the hotspot clients in connection with the API and the use of the API primitives mentioned above are described in the following in connection with Figs. 2 to
20 6.

Fig. 2 shows a message sequence chart of the registration of a hotspot client, in this example, of the WLAN hotspot client 1. For example, this registration procedure may be
25 carried out at the first time the network device connects to the particular hotspot, or beforehand via a website of the operator of the hotspot. Alternatively, the registration could be carried out when the hotspot client software is installed. It could be upon the first
30 connection or beforehand. The registration could also be done as part of the software build process by the manufacturer of the device.

The procedure starts with starting the installation
35 program of the WLAN hotspot client 2, in which the files

- 17 -

needed by the hotspot application are installed (step S1). In step S2, a register message "WLAN hotspot client 1" is sent to the operating system. In turn, the operating system records where the executable for "WLAN hotspot 1" is located and other configuration (step S3). As mentioned above, the hotspot client may be implemented as a dynamic link library, and upon the registration, the operating system learns the file name of the library.

10 After the "WLAN hotspot client 1" has been installed, it is possible to configure the operating system's setting for a certain profile to use "WLAN hotspot client 1". That is, the hotspot client is linked to a profile, as described above.

15

Fig. 3 shows a message sequence chart of an automatic hotspot login.

In step S11, the operating system (OS) detects a need to establish a WLAN connection to a network that is configured to use "WLAN hotspot client 1". After this, a layer 1 and 2 WLAN connection is established in step S12. In step S13 an Authenticate message is sent to the WLAN hotspot client 1. That is, this message is the API primitive by which the operating system can request the hotspot client to perform authentication, as described above.

The hotspot client 1 performs, in turn, an automatic login, using, e.g., HTTP (Hypertext Transfer Protocol), at an access point (not shown) of the corresponding hotspot (step S14). In case of a successful authentication, the WLAN hotspot client sends an Authentication complete (success) message to the operating system in step S15. This message is the API

- 18 -

primitive by which hotspot client can indicate to the operating system that the authentication has been successfully performed. In case of an unsuccessful case, the hotspot client 1 would send the API primitive
5 described above by which the hotspot client can indicate to the operating system that the authentication has failed.

After this, the operating system considers the WLAN
10 connection to be available and it can be indicated to the application or Mobile IP, for example (step S16). Thus, a full automatic hotspot login is performed, in which no further manual input from the user is necessary.

15 Fig. 4 shows a message sequence chart in which an automatic hotspot logoff is illustrated. An automatic hotspot logoff might be performed in order to save unnecessary login time or to save resources.

20 In step S21, the operating system detect that a WLAN connection needs to be closed. For example, no application is using the connection anymore. Thus, in step S22, it sends a Disconnect message to the WLAN hotspot client 1. This message is the API primitive
25 mentioned above by which the operating system can request the hotspot client to perform a de-authentication.

In turn, the WLAN hotspot client 1 performs a logoff protocol, e.g., by using HTTP (step S23). In case of a
30 successful de-authentication, it sends a De-authentication complete (success) message to the operating system in step S24. This message is the API primitive mentioned above by which the hotspot client can indicate to the operating system that the de-
35 authentication has been successfully performed. In case

- 19 -

of an unsuccessful de-authentication, the API primitive is sent, by which the hotspot client can indicate to the operating system that the de-authentication has failed.

- 5 In step S25, the operating system shuts down the WLAN layer 1 and 2 connection (established in step S12 shown in Fig. 3). Thereafter, the WLAN connection is closed.

10 In Fig. 5, a message sequence chart is shown illustrating a WLAN availability discovery and authentication.

In step S31, the WLAN hotspot client 1 sends a message Register for WLAN scanning results to the operating system. This is the API primitive mentioned above by
15 which the hotspot client can request the operating system to notify when a certain connection profile becomes available.

In turn, the operating system and the WLAN subsystem (3a
20 in Fig. 1) perform periodic scanning (step S32). In step S33, the operating system sends raw WLAN scanning results to the hotspot client. Then, the WLAN hotspot client uses its own network discovery settings (e.g., SSID lists) to detect whether a compatible network is available (step
25 S34). The hotspot client may use additional proprietary means to learn more about the WLAN networks. In case of success, the hotspot client sends a message including an Indication that a compatible WLAN hotspot is available to the operating system in step S35. In response to this,
30 the operating system decides to activate a WLAN hotspot connection with this compatible WLAN hotspot in step S36. In step S37, the automatic logon is carried out, as described above in connection with Fig. 3.

- 20 -

In Fig. 6, also a message sequence chart illustrating a WLAN availability discovery and authentication is shown, however, in this case the operating system manages the discovery settings.

5

In step S41, the operating system and the WLAN subsystem perform periodic scanning. In step S42, the operating system uses its own network WLAN discovery settings (e.g., SSID lists) to detect that a WLAN hotspot profile is available. In this step, the operating system may send the API primitive described above to the hotspot client by which the operating system can request the hotspot client to notify when a certain connection profile becomes available.

15

In case of success, the operating system decides in step S43 to activate the WLAN hotspot connection. Thereafter, the automatic logon described above in connection with Fig. 3 follows.

20

Thus, according to the present embodiment, a 'standard' API is created into the connection mechanism to automate hotspot login. This API is able to call external mechanisms, such as 802.1x mechanisms or proprietary authentication scripts so that users would need to perform minimal steps to use hotspots.

25

This API is tightly integrated into the WLAN connection management system in handhelds.

30

Hence, it is not necessary for the user to launch specialized software separately to access hotspots, and a common look & feel across multiple service providers is possible.

35

- 21 -

In the following, the WLAN hotspot authentication scenarios described above are described in more detail by referring to Figs. 7 to 9.

- 5 Fig. 7 shows a message sequence chart illustrating a basic middleware enabled hotspot authentication.

In principle, this is a more detailed procedure as described above in connection with Fig. 3. In particular,
10 Fig. 3 shows some more functions of the operating system, namely the WLAN subsystem, a network subsystem and a bearer manager. The procedure may start when some application or subsystem initiates a network connection. Then, the network subsystem sends a Connect message to
15 the WLAN subsystem. In this way, the WLAN layer 1 and 2 connection is established (similar to step S12 in Fig. 3). It is noted that before authentication, no IP-level connection up and data is allowed to flow to application.

- 20 The network subsystem selects a profile 1 and sends a message Connect Complete (profile 1) to the bearer manager, which forwards an Authentication (profile 1) to the WLAN hotspot client. That is, this message is the API primitive by which the operating system can request the
25 hotspot client to perform authentication (similar to step S13 in Fig. 3). Thereafter, the WLAN hotspot client performs the authentication by sending a HTTP request to the network subsystem, which sends a data request to the WLAN subsystem, which transmits the data to the hotspot.
30 A corresponding response is received via the WLAN subsystem and forwarded to the network subsystem, which sends a HTTP response to the WLAN hotspot client. This procedure corresponds to step S14 of Fig. 3. It is noted that the authentication by using HTTP is only an example.

- 22 -

Moreover, there may be more than only one or two transactions during the authentication.

5 In case of a successful authentication, an Authentication complete (success) message is sent to the bearer manager. This is the API primitive by which the hotspot client can indicate to the operating system that authentication has been successfully performed (similar to step S15 in Fig. 3).

10

After this, a Release connection (profile 1) is sent to the networking subsystem in order to release the connection after the successful connection. Thereafter, the connection is up and running. Data requests from the application are allowed to the network subsystem.

15

Fig. 8 shows a message sequence chart illustrating how discovery and authentication could be combined into a single operation.

20

The procedure starts when an application registers for connection availability regarding one or more profiles (profile 1, profile 2, ... profile n) with the bearer manager. The bearer manager sends a WLAN connection availability requested indication message to the WLAN hotspot client. In turn, the WLAN hotspot client may request priority availability indications for all the supported connection profiles and sends a corresponding message Register for priority connection availability (profile 1, profile 4, ...), assuming that profile 1 has the highest priority, profile 4 as the second highest priority and so on.

25

30

Meanwhile, the WLAN subsystem performs periodic scanning, and send a Scan response including a station list. The

35

- 23 -

bearer manager checks whether there is a matching WLAN network. In case a matching WLAN network is found, a connection availability indication (profile 1) is sent to the WLAN hotspot client, assuming that a network
5 corresponding to profile 1 is available. The WLAN hotspot client sends then a Connect (profile 1) to the networking subsystem, so that then a WLAN authentication is performed according to the scheme as shown in Fig. 7. Thereafter, a connection to profile X (e.g., profile 1 as
10 described above) available indication is sent to the WLAN hotspot, which sends a Connect (profile X) to the bearer manager.

Fig. 9 shows a message sequence chart illustrating a WLAN
15 hotspot de-authentication.

Similar as described above in connection with Fig. 4, the de-authentication may start when some application or subsystem initiates a disconnect request to shutdown the
20 connection, for example, when it is discovered that the connection is no longer needed.

Thus, the networking subsystem issues a disconnect indication (profile 1) to the bearer manager, which sends
25 a Disconnect (profile 1) to the WLAN hotspot client. That is, this is the API primitive by which the operating system can request the hotspot client to perform de-authentication (similar to step S22 in Fig. 4). The hotspot client performs the logoff by using HTTP, similar
30 as in the case of performing the authentication (similar to step S23 in Fig. 4). It is noted that performing the de-authentication by using HTTP is only an example. Moreover, there may be more than one or two transactions during the de-authentication.

35

- 24 -

When the de-authentication has been successful, the WLAN hotspot client sends a de-authentication complete (success) message to the bearer manager. This is the API primitive by which the hotspot client can indicate to the operating system that the de-authentication has been successfully performed (similar to step S24 in Fig. 4). The bearer manager sends a corresponding message shutdown connection 8profile 1) to the networking subsystem, which issues a shutdown WLAN connection message to the WLAN subsystem.

Thereafter, the connection is down and no data even at link layer can be exchanged anymore.

Thus, according to the present embodiment, it is possible to implement 3rd party hotspot logon clients, which improve the usability of public WLAN. In particular, the operating system has the knowledge about which profiles are available, which networks (SSIDs). This information is used by the hot spot clients to do the authentication.

That is, according to the embodiment, integration of 3rd party hotspot clients with native user interfaces, automatic connection selection, and seamless roaming are possible.

Hence, this invention enables seamless roaming when there are several higher layer (higher than link layer) authentications needed, for example, when several hotspot clients are used. This is possible due to the automatic authentication.

In particular when a WLAN hotspot client is implemented on a mobile device, such as a Symbian phone, the

- 25 -

following advantages are achieved according to the invention:

- 5 - A 3rd party application is enabled to manage its own WLAN settings, compatibly with the existing WLAN Internet Access Point definition. The existing middleware should be able to detect when a WLAN hotspot connection is available.
- 10 - WLAN hotspot clients are integrated with the device's connection selection user interfaces, with automatic Internet Access Point selection and with seamless roaming.
- 15 - the user does not need to run a hotspot client separately before running the actual application that the user wants to use. Instead, the hotspot application can be run automatically when needed.

20 The invention is not limited to the embodiment described above, and various modifications are possible.

For example, the invention is not limited to WLAN, but can also be applied to other connection networks such as Bluetooth, WiMAX and the like in which it is possible to connect to different access entities which may have
25 different profiles and it is necessary to perform an authentication. That is, the access client (hotspot client) could be any authentication client that performs an authentication task before the connection is "released" to other applications.

30 Moreover, it is not even necessarily restricted to radio networks, it is also applicable to wired networks, when a connection to an network access entity is achieved via a wired access point by using a cable (such as a LAN

- 26 -

connection or the like). In this case, different specifications of the wired access point can be considered by using different access clients. For example, the present invention can be applied to xDSL or
5 other wired broadband connections.

Moreover, in the above description of the preferred embodiment, the "hotspot" is only an example for a network access entity. That is, also other forms of a
10 network access entity are possible.

Furthermore, according to the embodiment described above, the WLAN hotspot client (as an example for an access client entity) and the operating system (as an example
15 for an operation entity) are implemented as software within a computer running the network device. However, the access client entity and the operation entity may also be realized as hardware such as ASICs, DSPs or the like, so that different access client entities may also
20 be replaced or used by inserting corresponding components into a suitable socket or the like of the network device.

- 27 -

CLAIMS

1. A method for handling a network connection of a network device comprising an operation entity (3) for
5 handling network connection, wherein at least one access client entity (1, 2) providing connection handling to a specific network access device is connectable to the operation entity, the method comprising the steps of
10 identifying (S11), by the operation entity, a need for a network connection,
requesting (S13) the access client entity to perform authentication, and
performing (S14), by the access client entity, the authentication.
15
2. A method for operating an operation entity (3) for handling network connection, wherein at least one access client entity (1, 2) providing connection handling to a specific network access device is connectable to the
20 operation entity, the method comprising the steps of
identifying (S11), by the operation entity, a need for a network connection, and
requesting (S13) the access client entity to perform authentication.
- 25
3. A method for operating an access client entity for handling a network connection to a specific network access device, connectable to a network device comprising an operation entity (3) for handling network connection,
30 the method comprising the steps of
receiving (S13) a request from the operation entity (3) to perform authentication, and
performing (S14) the authentication.

- 28 -

4. The method according to one of the claims 1 to 3,
further comprising the step of

informing (S15) the operation entity about the
result of the authentication by the access client entity,

5 and,

in case the authentication was successful, allowing
(S16), by the operation entity, use of the network
connection.

10 5. The method according to one of the claims 1 to 3,
wherein a plurality of access client entities is
provided, and the identifying step (S11) comprises the
step of selecting an access client entity of the
plurality of access client entities based on the need for
15 a network connection.

6. The method according to one of the claims 1 to 3,
wherein a message is sent from the access client entity
to the operating system client to request the operating
20 system client to notify when a certain connection profile
becomes available.

7. The method according to one of the claims 1 to 3,
wherein a message is sent from the operating system
25 client to the access client entity to request the access
client entity to notify when a certain connection profile
becomes available.

8. The method according to one of the claims 1 to 3,
30 wherein a message is sent from the operation entity to
the access entity client by which the operation entity
requests the access client entity to perform the
authentication.

- 29 -

9. The method according to one of the claims 1 to 3,
wherein a message is sent from the operation entity to
the access entity client by which the operation entity
requests the access client entity to perform a de-
5 authentication.

10. The method according to one of the claims 1 to 3,
wherein a message is sent from the access client entity
to the operation entity by which the access client entity
10 indicates to the operating system that the authentication
has been successfully performed.

11. The method according to one of the claims 1 to 3,
wherein a message is sent from the access client entity
15 to the operation entity by which the access client entity
indicates to the operating system that de-authentication
has been successfully performed.

12. The method according to one of the claims 1 to 3,
20 wherein a message is sent from the access client entity
to the operation entity by which the access client entity
indicates to the operating system that authentication/de-
authentication has failed.

25 13. The method according to one of the claims 1 to 3,
further comprising the step of
prohibiting a modification of a network connection
setting by a user input.

30 14. The method according to one of the claims 1 to 3,
further comprising the step of
registering an access client entity to the operation
entity.

- 30 -

15.. The method according to one of the claims 1 to 3,
further comprising the step of

linking an access client entity to a profile,
wherein in the authenticating step, the operation entity
5 informs the access client entity linked to the profile in
case a connection with the profile is to be established.

16. A network device comprising an operation entity (3)
for handling network connection and at least one access
10 client entity (1, 2) providing connection handling to a
specific network access device, wherein

the operation entity is adapted to identify a need
for a network connection and to inform the access client
entity, and

15 the at least one access client entity is adapted to
perform an authentication.

17. The network device according to claim 16, wherein
the access client entity (1, 2) is adapted to inform the
20 operation entity about the result of the authentication
by the access client entity, and the operation entity is
adapted to, in case the authentication was successful,
allow use of the network connection.

25 18. The network device according to claim 16, wherein a
plurality of access client entities is provided, and the
operation entity is adapted to select an access client
entity of the plurality of access client entities based
on the need for a network connection.

30 19. The network device according to claim 16, wherein
the access client entity is adapted to send a message to
the operation entity to request the operation entity to
notify when a certain connection profile becomes
35 available.

- 31 -

20. The network device according to claim 16, wherein the operation entity is adapted to send a message to the access client entity to request the access client entity
5 to notify when a certain connection profile becomes available.

21. The network device according to claim 16, wherein the operation entity is adapted to send a message to the
10 access entity client by which the access client entity is requested to perform the authentication.

22. The network device according to claim 16, wherein the operation entity is adapted to send a message to the
15 access entity client by which the access client entity is requested to perform a de-authentication.

23. The network device according to claim 16, wherein the access client entity is adapted to send a message to
20 the operation entity indicating that the authentication has been successfully performed.

24. The network device according to claim 16, wherein the access client entity is adapted to send a message to
25 the operation entity indicating that de-authentication has been successfully performed.

25. The network device according to claim 16, wherein the access client entity is adapted to send a message to
30 the operation entity indicating that authentication/de-authentication has failed.

26. The network device according to claim 16, wherein the operation entity is adapted to prohibit a

- 32 -

modification of a network connection setting by a user input.

27. The network device according to claim 16, wherein
5 the operation entity is adapted to register an access client entity.

28. The network device according to claim 16, wherein
10 the operation entity is adapted to link an access client entity to a profile, wherein the operation entity is adapted to inform the access client entity linked to the profile in case a connection with the profile is to be established.

15 29. An access client entity [KJ2]providing connection handling for a specific network access device, comprising means for receiving a request to perform authentication from an operation entity, and means for performing the authentication.

20

30. The access client entity according to claim 29, further comprising means for informing the operation entity [KJ3]y about the result of the authentication.

25 31. The access client entity according to claim 29, further comprising means for sending a message to the operation entity to request the operation entity to notify when a certain connection profile becomes available.

30

32. The access client entity according to claim 29, further comprising receiving means for receiving a message requesting the access client entity to notify when a certain connection profile becomes available.

35

- 33 -

33. The access client entity according to claim 29, further comprising receiving means for receiving a message by which the access client entity is requested to perform the authentication.

5

34. The access client entity according to claim 29, further comprising receiving means for receiving a message by which the access client entity is requested to perform a de-authentication.

10

35. The access client entity according to claim 29, further comprising a sending means for sending a message to the operation entity indicating that the authentication has been successfully performed.

15

36. The access client entity according to claim 29, further comprising a sending means for sending a message to the operation entity indicating that de-authentication has been successfully performed.

20

37. The access client entity according to claim 29, further comprising a sending means for sending a message to the operation entity indicating that authentication/de-authentication has failed.

25

38. The access client entity according to claim 29, further comprising means for registering to the operation entity.

30 39. An operation entity (3) for handling network connection, the operation entity (3) comprising means for identifying a need for a network connection, and

- 34 -

means to request an access client entity (1, 2) providing connection handling for a specific network access device to perform an authentication.

- 5 40. The operation entity according to claim 39, further comprising means for receiving an authentication result, and means for allowing use of the network connection in case the authentication was successful.
- 10 41. The operation entity according to claim 39, further comprising means for selecting an access client entity of a plurality of access client entities based on the need for a network connection.
- 15 42. The operation entity according to claim 39, further comprising receiving means for receiving a message requesting to notify when a certain connection profile becomes available.
- 20 43. The operation entity according to claim 39, further comprising sending means for sending a message to the access client entity requesting to notify when a certain connection profile becomes available.
- 25 44. The operation entity according to claim 39, further comprising sending means for sending a message to the access client entity requesting the access client entity to perform the authentication.
- 30 45. The operation entity according to claim 39, further comprising sending means for sending a message to the access client entity requesting the access client entity to perform a de-authentication.

- 35 -

47. The operation entity according to claim 39, further comprising a receiving means for receiving a message indicating that the authentication has been successfully performed.

5

47. The operation entity according to claim 39, further comprising a receiving means for receiving a message indicating that a de-authentication has been successfully performed.

10

48. The operation entity according to claim 39, further comprising a receiving means for receiving a message indicating that an authentication or de-authentication has failed.

15

49. The operation entity according to claim 39, further comprising means for prohibiting a modification of a network connection setting by a user input.

20

50. The operation entity according to claim 39, further comprising means for registering an access client entity.

25

51. The network device according to claim 39, further comprising means for linking an access client entity to a profile, wherein the operation entity is adapted to inform the access client entity linked to the profile in case a connection with the profile is to be established.

30

52. A computer program product for a computer, comprising software code portions for performing the steps of any one of claims 1 to 15 when the program is run on the computer.

35

53. The computer program product according to claim 51, wherein the computer program product comprises a

- 36 -

computer-readable medium on which the software code portions are stored.

54. The computer program product according to claim 51,
5 wherein the computer is a part of the network device.

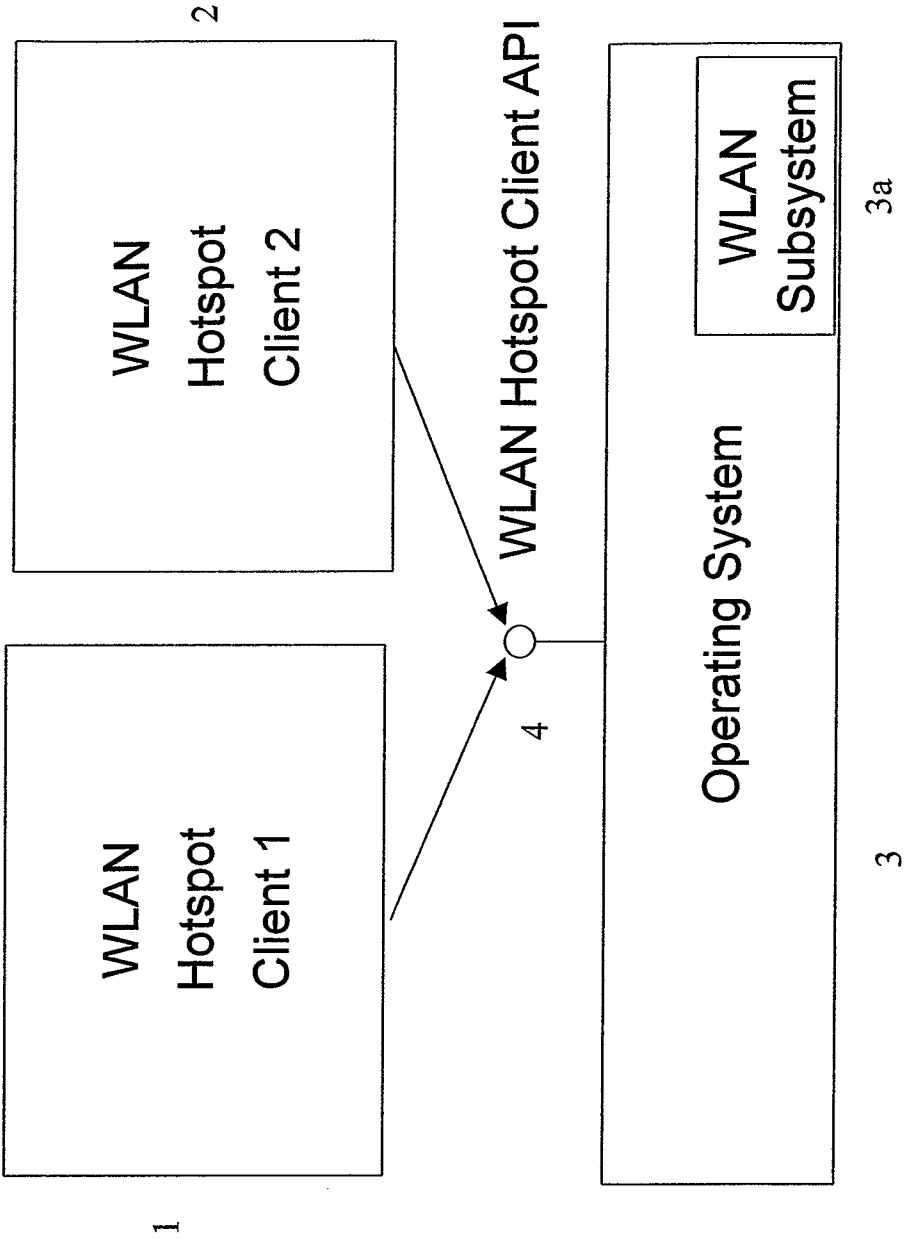


Fig. 1

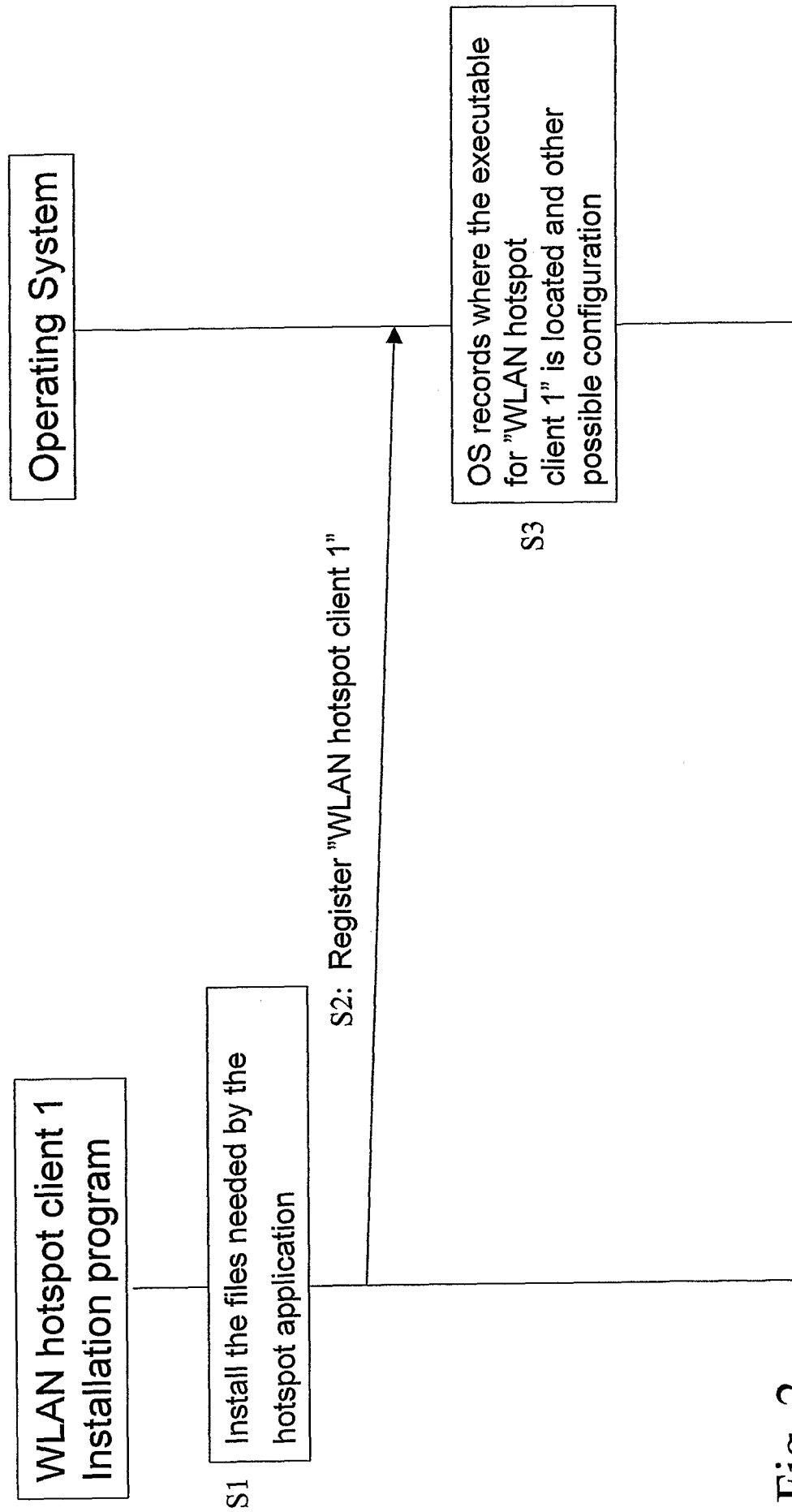


Fig. 2

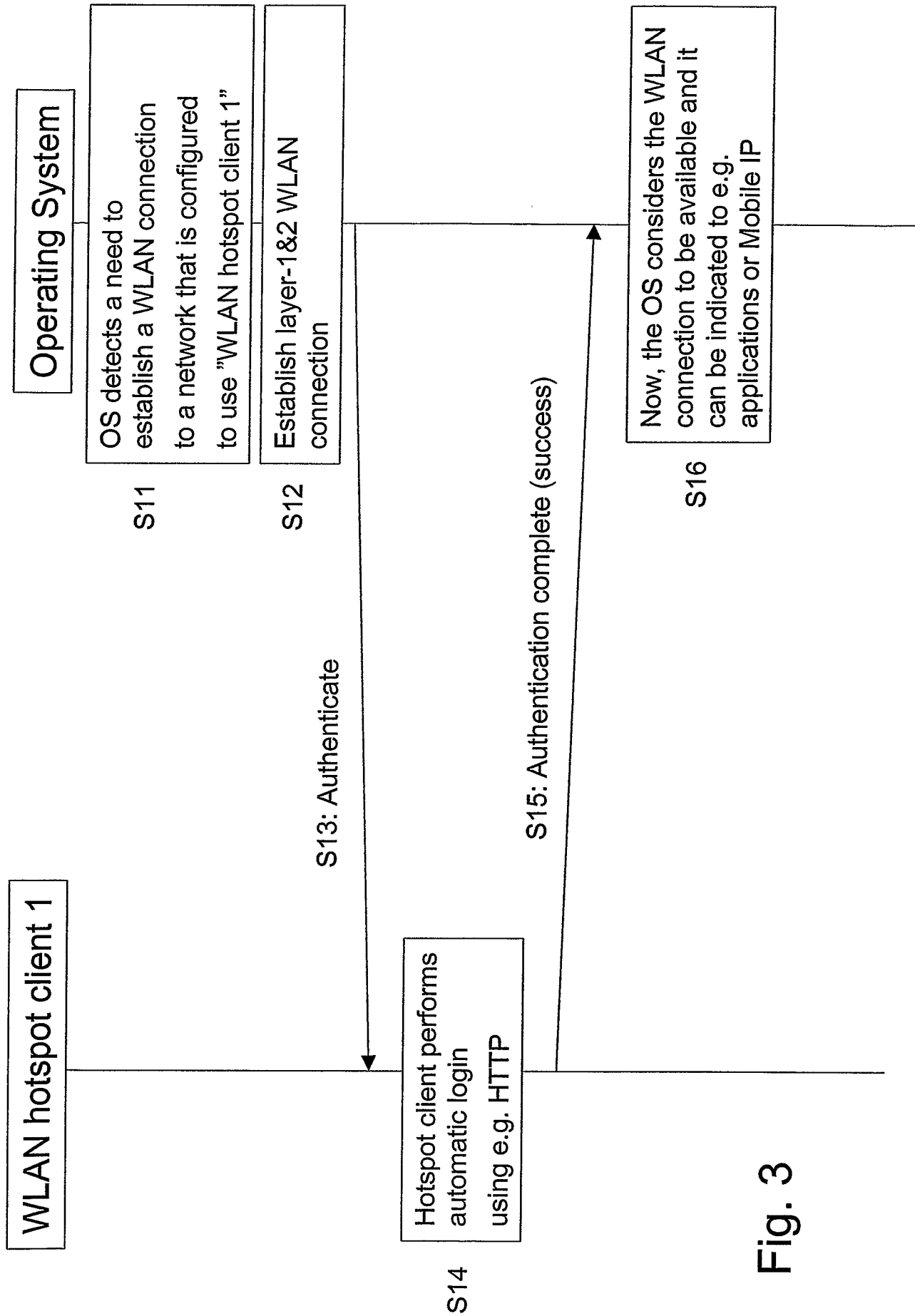


Fig. 3

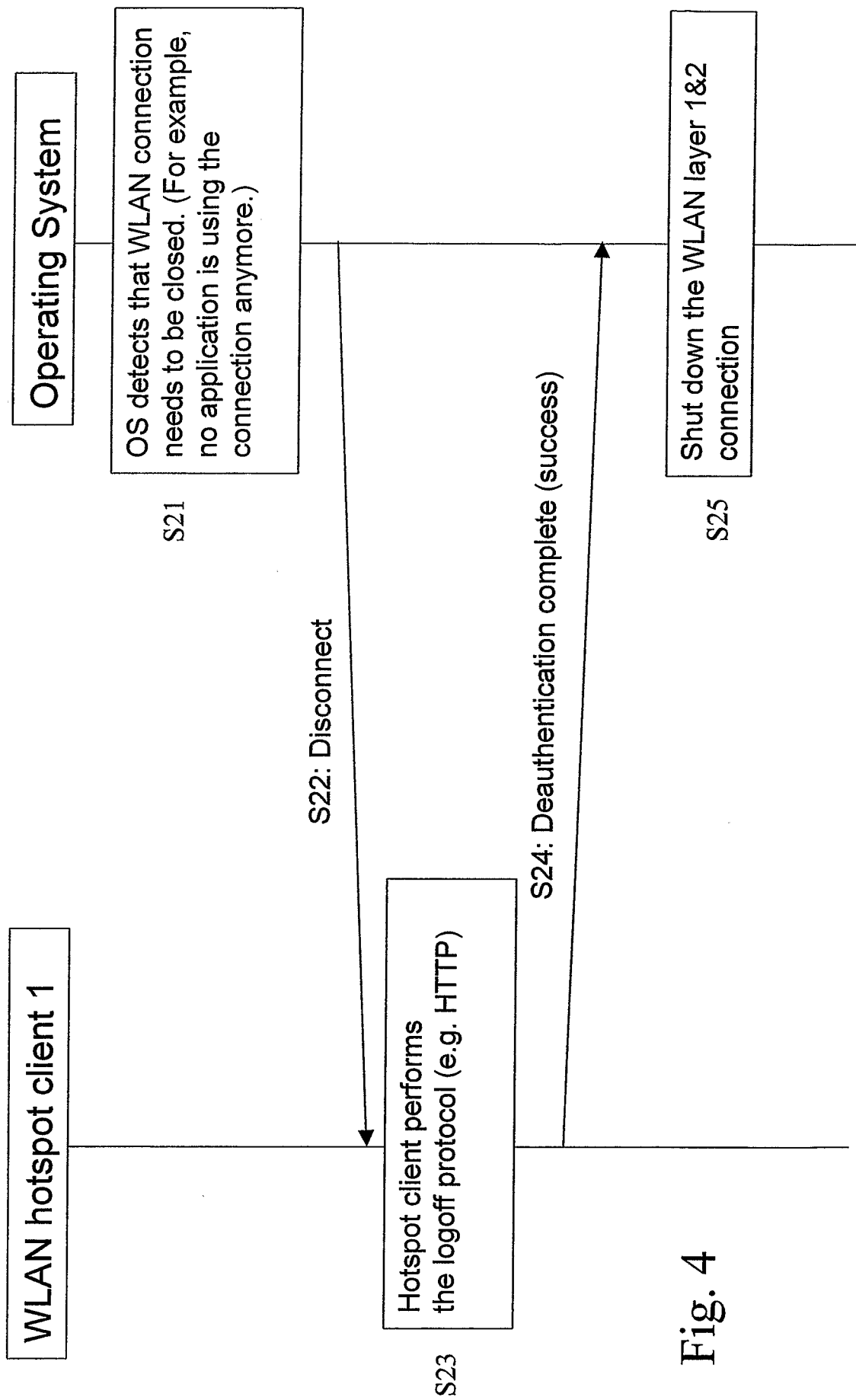


Fig. 4

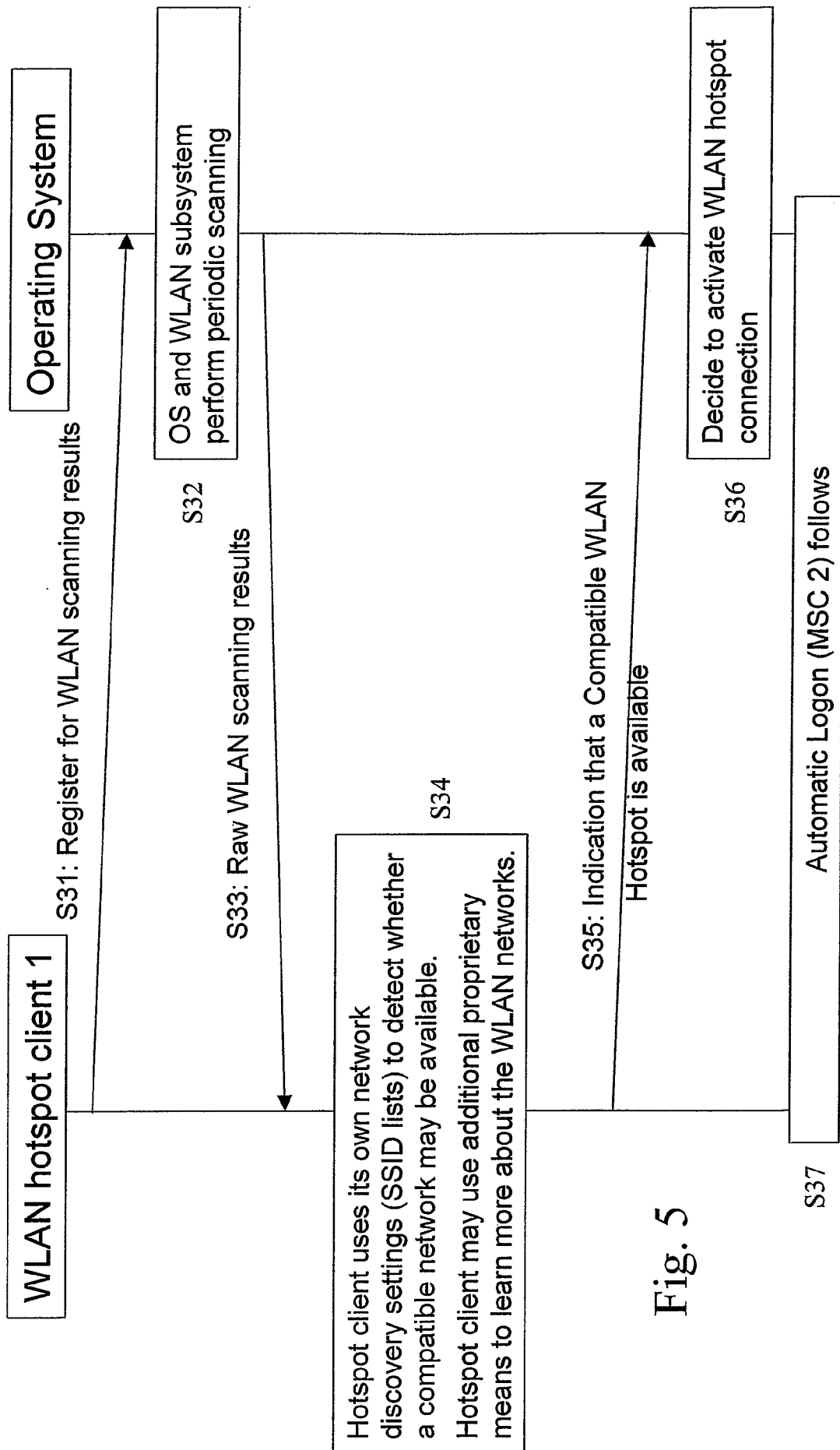


Fig. 5

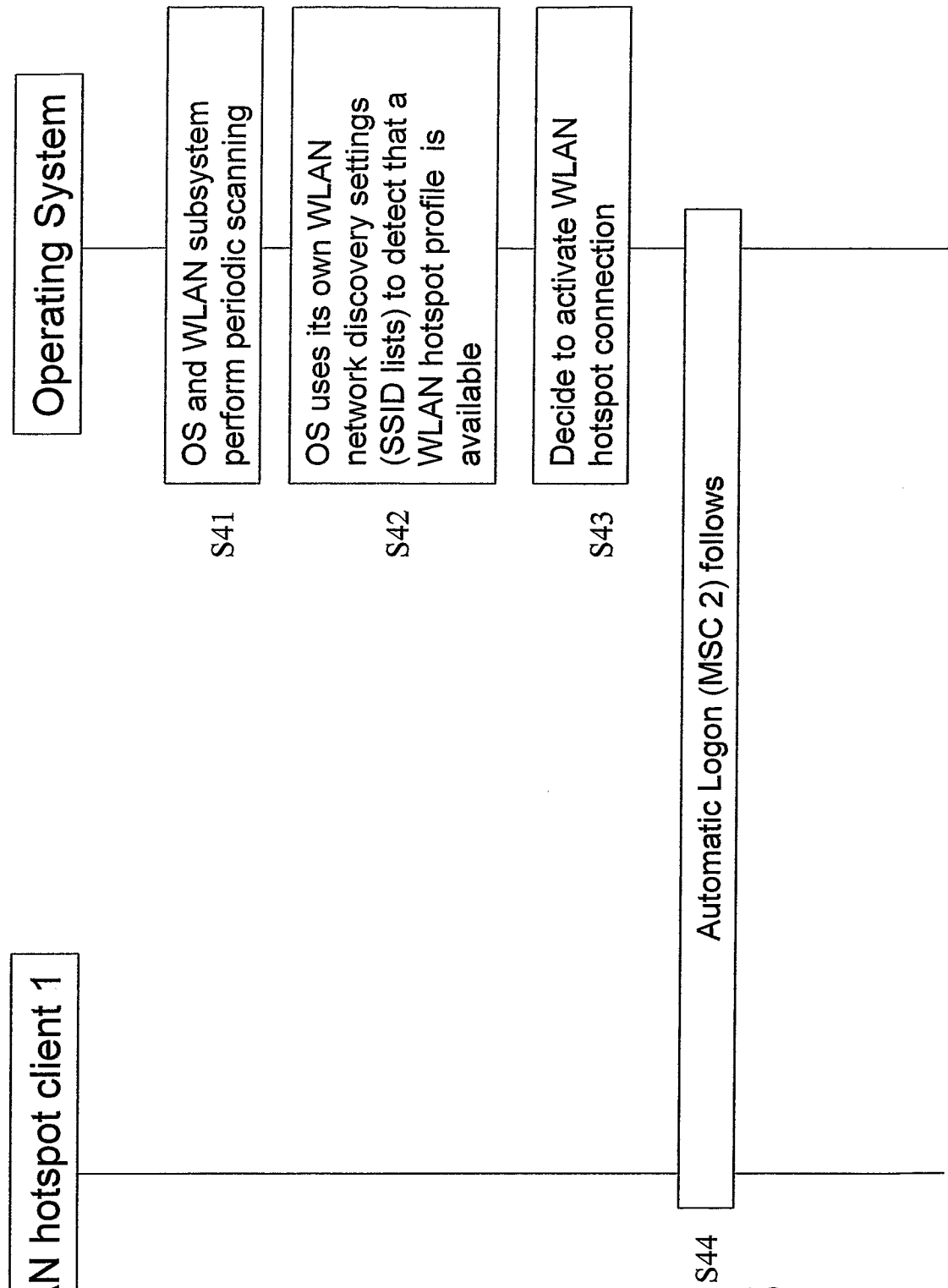


Fig. 6

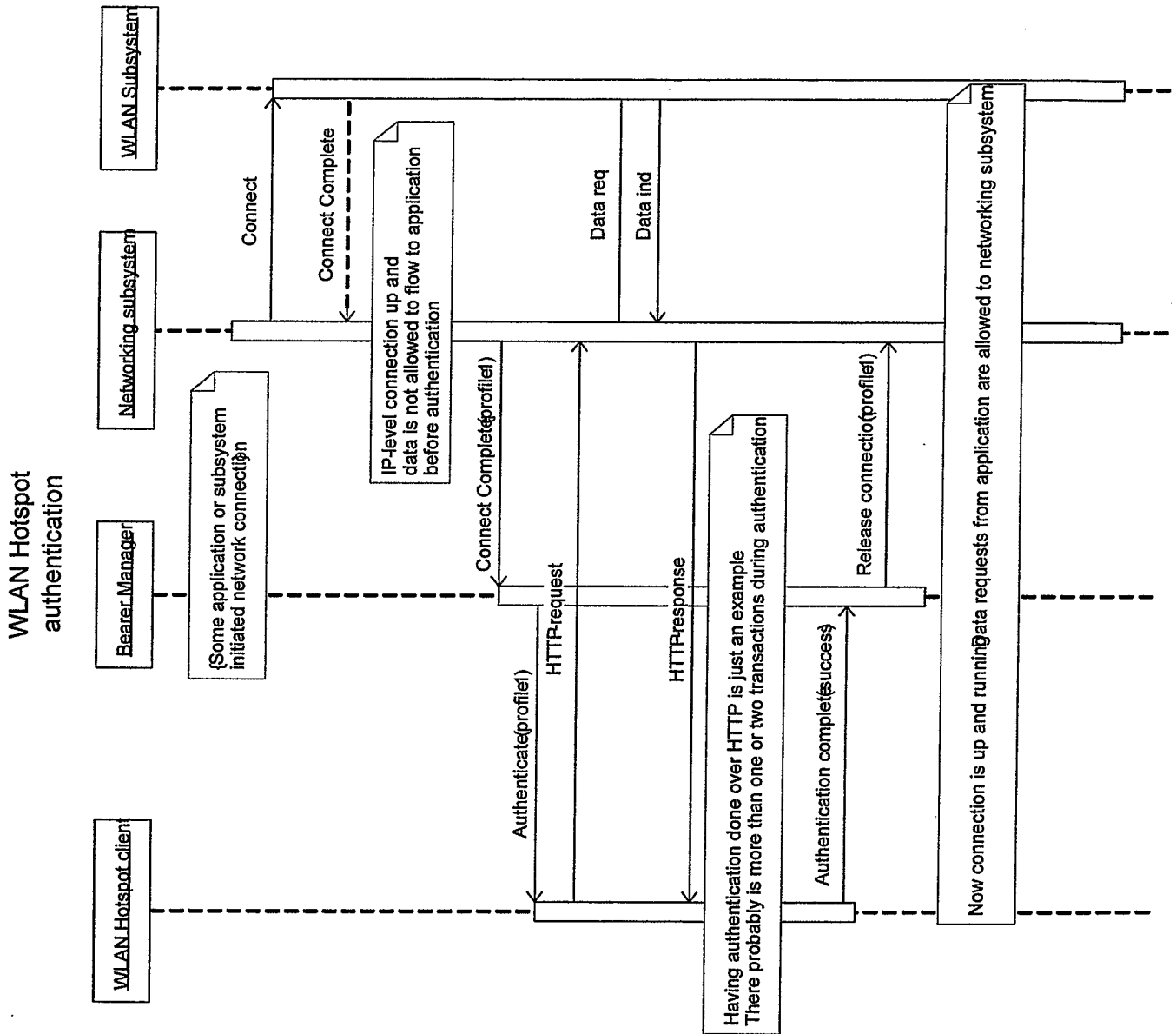


Fig. 7

WLAN availability discovery and authentication

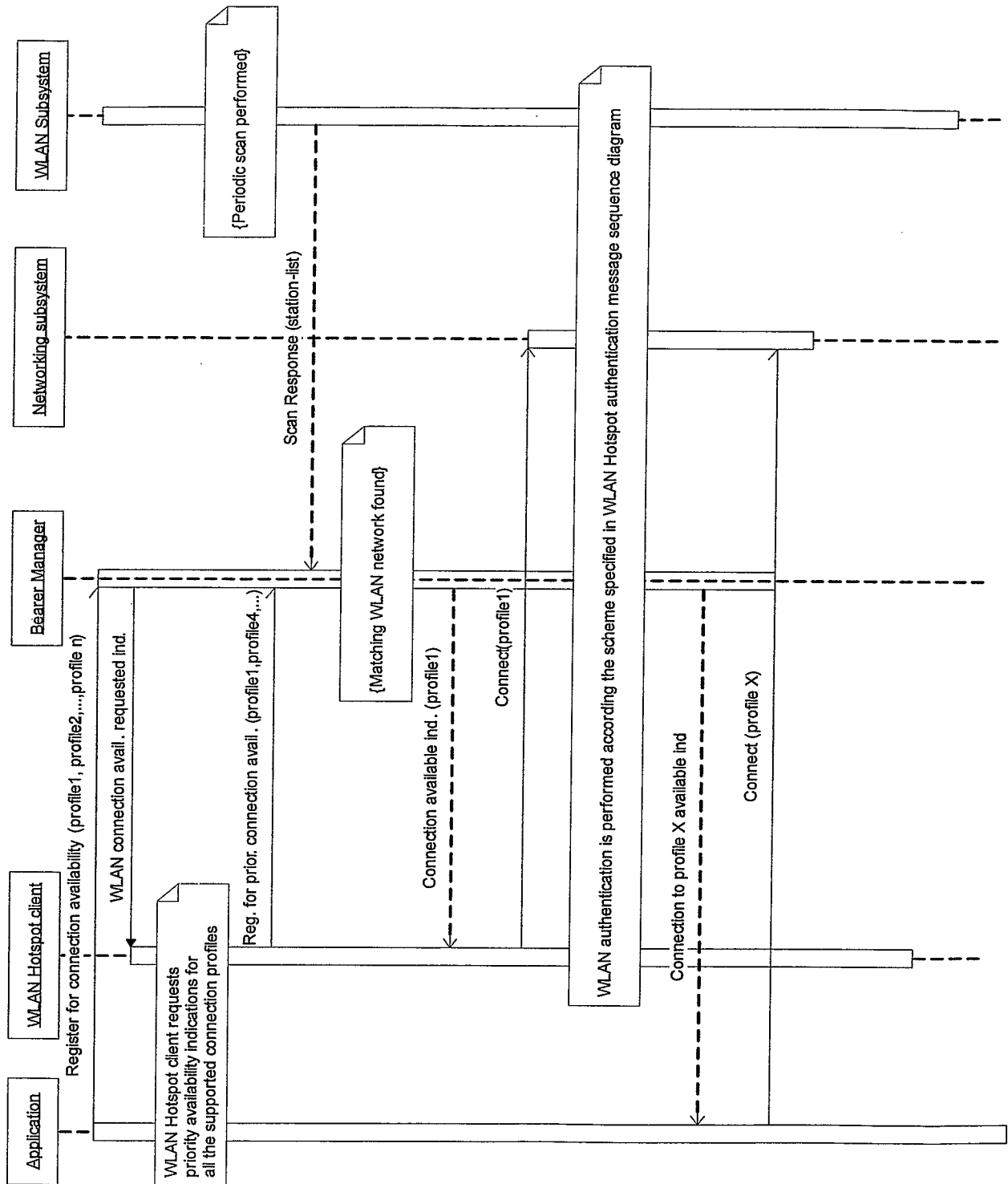


Fig. 8

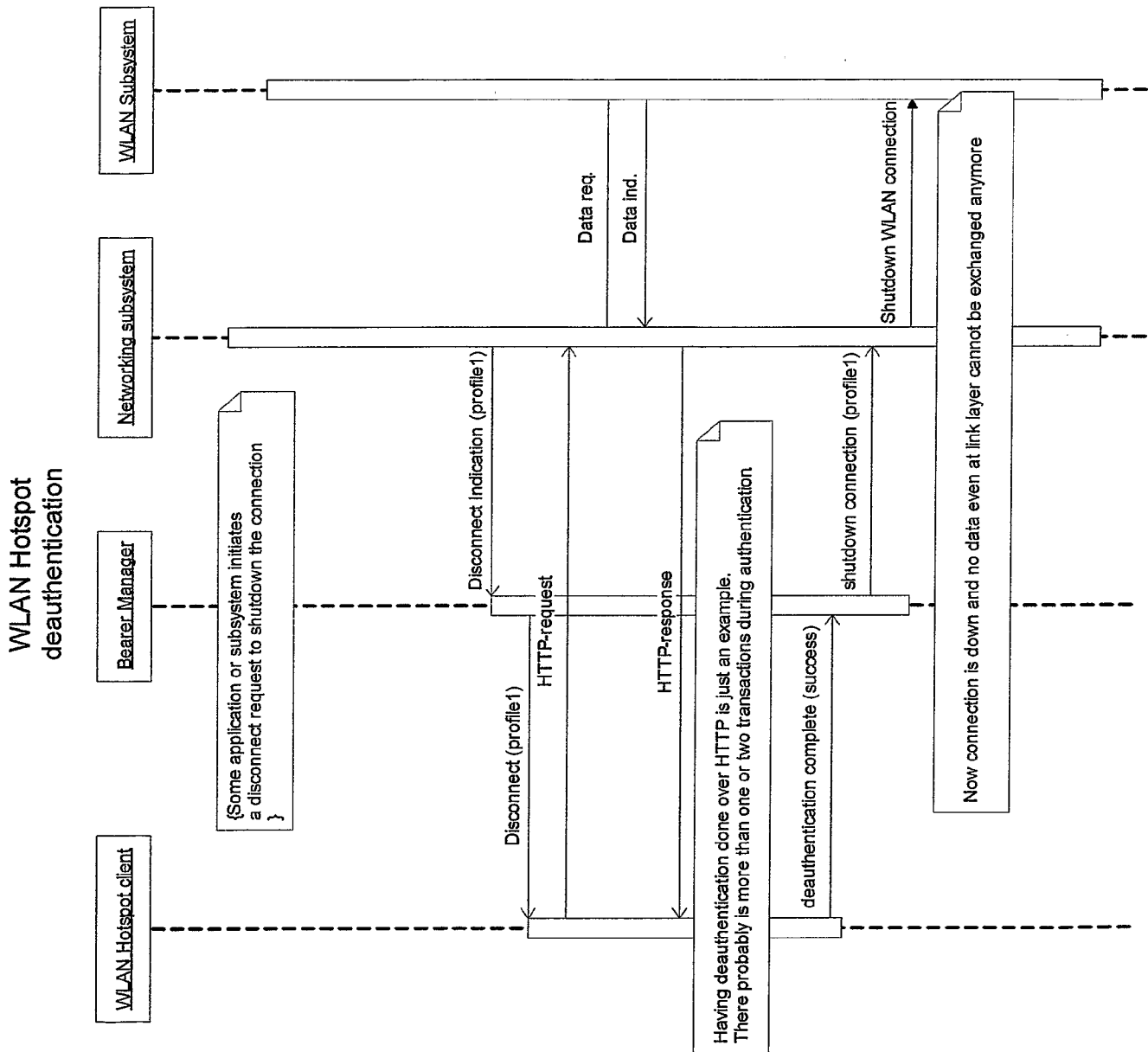


Fig. 9

INTERNATIONAL SEARCH REPORT

International application No

PCT/IB2005/003807

A. CLASSIFICATION OF SUBJECT MATTER

H04L29/06

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)

H04L G06F

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 practical, search terms used)

EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	WO 00/49505 A (HENDRICK, COLIN) 24 August 2000 (2000-08-24) page 3, line 9 - page 5, line 2 page 5, line 31 - page 6, line 35 page 8, line 3 - page 9, line 10 page 11, line 18 - page 13, line 25 page 14, line 18 - page 15, line 24 ----- -/--	1-4, 8-14,16, 17, 21-27, 29,30, 33-41, 44-50, 52-54 5-7,15, 18-20, 28,31, 32,42, 43,51

☒ Further documents are listed in the continuation of Box C.☒ 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 document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which 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

10 March 2006

Date of mailing of the international search report

17/03/2006

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Olachea, F

INTERNATIONAL SEARCH REPORT

International application No

PCT/IB2005/003807

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2004/068653 A1 (FASCENDA ANTHONY C) 8 April 2004 (2004-04-08) paragraphs '0011! - '0015! paragraphs '0018! - '0022! paragraphs '0042! - '0045! paragraphs '0051! - '0054! paragraphs '0066! - '0078! -----	1-54
A	US 2005/195778 A1 (BERGS MAGNUS H ET AL) 8 September 2005 (2005-09-08) paragraphs '0013! - '0020! paragraphs '0027! - '0036! -----	1-54
A	US 2005/163319 A1 (HANCOCK ROBERT ET AL) 28 July 2005 (2005-07-28) paragraphs '0005! - '0007! paragraphs '0017! - '0023! -----	1-54

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/IB2005/003807

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 0049505	A	24-08-2000	NONE	
US 2004068653	A1	08-04-2004	NONE	
US 2005195778	A1	08-09-2005	DE 10341873 A1 WO 2005024543 A2	07-04-2005 17-03-2005
US 2005163319	A1	28-07-2005	AU 2004224971 A1 CA 2486226 A1	26-05-2005 07-05-2005