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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 September 2001 (07.09.2001)

PCT

(10) International Publication Number
WO 01/65380 A1

(51) International Patent Classification[7]: G06F 13/00, 13/14, 15/16, G09C 3/00, G06F 1/26

(21) International Application Number: PCT/US01/06143

(22) International Filing Date: 27 February 2001 (27.02.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/185,655 29 February 2000 (29.02.2000) US

(71) Applicant: IPRIVACY LLC [US/US]; 599 Lexington Avenue, New York, NY 10022 (US).

(72) Inventors: STOLFO, Salvatore, J.; 80 Kenilworth Road, Ridgewood, NJ 07450 (US). SMITH, Jonathan; 771 Princeton-Kingston Road, Princeton, NJ 08540-4165 (US).

(74) Agents: MORRIS, Francis, E. et al.; Pennie & Edmonds LLP, 1155 Avenue of the Americas, New York, NY 10036 (US).

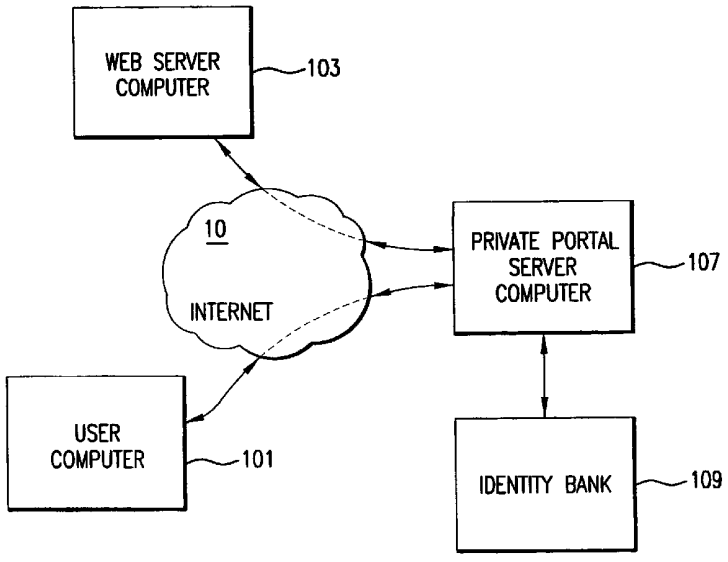
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, 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: ANONYMOUS AND PRIVATE BROWSING OF WEB-SITES THROUGH PRIVATE PORTALS



(57) Abstract: A method and apparatus for enabling a user having a first identification at a first computer to (101) communicate privately with a second computer (103). The method includes the step of receiving from the first computer (101) a request to send a first message to the second computer (103), assigning a second identification to the user, and forwarding the first message to the second computer (103) using the second identification. The method further includes the steps of receiving a second message from the second computer (103) in response to the first message, and forwarding the second message to the first computer (101) using the first identification. A corresponding system is also described.

WO 01/65380 A1

ANONYMOUS AND PRIVATE BROWSING OF WEB-SITES THROUGH PRIVATE PORTALS

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority to United States Provisional Application No. 60/185,655 filed February 29, 2000. A co-pending United States Patent Application No. 09/360,812, entitled "Electronic Purchase of Goods over a Communication Network Including Physical Delivery While Securing Private and Personal Information of the Purchasing Party" by Stolfo, et al., filed July 26, 1999 is incorporated herein by reference.

FIELD OF THE INVENTION

The present invention relates to a Web server configured to provide anonymous and private browsing of Web sites.

BACKGROUND OF THE INVENTION

It is common practice today for retailers, merchants and marketers to collect data on users of the Internet, and to merge the collected data from multiple sources to "data mine" or learn about the users' identities and their private/personal information in order to target them for advertising or other purposes. Internet surfing habits of users are also gathered in order to "personalize" their Web experience.

Private information as used in the present invention is a broad concept. For instance, the private information may include name, email address, login name, postal address, IP address, phone number, financial information, "click stream" behavior, or purchasing behavior or other information attributable to individual users. To prevent the above described unwanted intrusion on privacy, a number of conventional Web servers provide anonymous Internet browsing features. Referring to FIG. 1, a user at a user computer 11 wishing to browse Web pages provided by a Web server 13 can first download a Web page provided by a conventional anonymous server computer 15. The user then can access the Web pages of Web server 13 through anonymous server computer 15 without revealing his/her true identity by using a proxy identification provided by anonymous server

computer 15. However, in the conventional systems, Web server 13 cannot send any customized or individualized information back to the user. For instance, if Web server 13 provides research information on certain subjects not regularly available in the Web pages provided by Web server 13, then no such research data can be forwarded to the user because Web server 13 only has the proxy identification provided by anonymous server computer 15 but does not have the true identification to send such information to the user. Further, anonymous server computer 15 does not keep any information to map the proxy identification back to the true identification of its users. For the same reason, if the user wishes to purchase goods and/or services from the company operating Web server 13, the user either has to reveal his/her true identity to Web server computer 13 or cannot purchase the goods and/or services.

SUMMARY OF THE INVENTION

The present invention provides for browsing Web pages provided by a Web server computer anonymously and privately. Further, the present invention allows messages to be exchanged between the user computer and the Web server computer. In particular, a trusted third party entity (*i.e.*, a private portal server computer) registers true identity information of a user (*e.g.*, e-mail addresses, IP address, URL, Web identification, etc.) and provides to the user a proxy identity for use when browsing the Web pages of the Web server computer. An example of a trusted third party is an accounting firm that may provide a legally binding and financially secured audit guarantee that the trusted third party will not disclose true identity information. The proxy identities may be retired or expunged when the user browses elsewhere after having extracted information from the Web server.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred features of the present invention are disclosed in the accompanying drawings, wherein similar reference numbers denote similar elements throughout the several drawings, and wherein:

FIG. 1. is a diagram illustrating a conventional system for accessing a Web server computer anonymously;

FIG. 2 is a diagram illustrating the preferred system of privately accessing a Web server computer;

FIG. 3 is a diagram illustrating another preferred system of privately accessing a Web server computer; and

FIG. 4 is a diagram illustrating an identity bank of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

FIG.2 depicts one or more user computers 101, one or more Web server computers 103 and a private portal server computer 107 that are interconnected by Internet 10. Private portal server computer 107 is a trusted third party. A user at user computer 101 can browse Web pages at Web server computer 103 anonymously and privately by sending a message to private portal computer 107 requesting that the Web pages at Web server computer 103 be downloaded to user computer 101. The request is made by user computer 101 using a true identification of the user (*e.g.*, e-mail addresses, IP addresses, URL, Web identifications, etc.). Further, the message is written in a browser language such as hypertext markup language (HTML), extensible markup language (XML) or other browser language available to one of ordinary skill in the art.

Upon receiving the message, portal server 107 assigns a proxy identification to the user using an identity bank 109. In particular, identity bank 109 maintains a table that matches identifications of many users and proxy identifications. Moreover, identity bank 109 provides for prompt retrieval of one type of identification in response to entry of the other type of identification. After a proxy identification has been assigned to the message from user computer 101, portal server 107 forwards the message to Web server 103 using the proxy identification. Once the above links are established among user computer 101, portal server computer 107 and Web server computer 103, the Web pages of Web server computer 103 can be browsed by the user anonymously. Further, additional messages can be exchanged among them.

Unlike the conventional system described above in connection with FIG. 1, the system described in FIG. 2 allows messages to be sent from Web server computer 103 to user computer 101 using the proxy identification. More specifically, messages from Web server 103 using the proxy identification as the messages' destination address are forwarded to portal server 107. At portal server 107, the proxy identifications are replaced with the true user identifications based on information stored in identity bank 109. After this replacement, the messages are then forwarded to user computer 101 using the true user

identification as the destination address. The messages from Web server 103 generated based on the request from the user may include research information on certain subjects not regularly available in the Web pages provided by Web server 103. More examples of these types of customized private messages are discussed later.

It should be noted that the above discussed system allows the user to remain anonymous while allowing the user to receive private messages from Web server 103.

It should also be noted that providing access to Web server 103 via private portal server 107 involves not only assigning proxy identities to users but also certifying that Web server 103 is visited anonymously. Thus, the trusted third party (*i.e.*, portal server 107) has a trust relationship with the user and the company operating Web server 103. However, there is no such trust relationship between the user and the company operating Web server 103. Furthermore, the trusted third party (*i.e.*, portal server 107) retains sufficient information about the true identity of the user so that any subsequent transaction can be accomplished readily between the user and Web server 103, using standard transaction media (*e.g.*, credit cards).

Private portal 107 is preferably implemented by a combination of existing technologies, and preferably requires no change to the form, structure and content of the Web pages of Web server 103. In one exemplary embodiment, the private portal server 107 includes an anonymizing server (*e.g.*, Anonymizer.com) or other anonymizing services commonly known in the art and identity bank 109.

In another embodiment, a user may directly access the Web site without first downloading web pages from the trusted third party. For instance, a user may access a Web page of www.irs.gov privately simply by browsing at www.private.irs.gov (or alternatively, www.irs.private.gov), an address maintained at private portal server 107 which passes the user's browser Web request through private portal server 107 on its way to the IRS' Web site after the browser request has been anonymized (*e.g.*, provided with a proxy identity). In fact, a user does not need to know whether a Web site he/she wishes to browse has a private portal or not. By using URL "name space" is such a general way, a user can simply type in www.private.XXX.com (or alternatively, www.XXX.private.com) and if a private portal does indeed exist, it would be automatically accessed by the user's Web browser. There would be no particular need to advertise the existence of the private portal if a standard private portal name as suggested here is used by each Web site provider.

In yet another embodiment, the private portal server service is preferably provided as a front end to an existing Web server (commercial or other) offering services or information to users of the Web. In other words, the "private portal" preferably offers specific features and functions provided by Web server 103, and serves as a private entry point to the Web site provider for customers who may want to remain anonymous. Thus, private portal server 107 can be easily and conveniently implemented on the World Wide Web at any Web site that wishes to provide a private portal to its particular Web site. It should be emphasized that the private portal server 107 does not provide a general Web site that users may pass through when visiting *any* other Web site. Server 107 is specific and specialized to a distinct Web site; it is not a single server that handles *all* Web sites (i.e., www.anonymizer.com).

More specifically, Web server 103 itself provides an option to browse its Web pages anonymously and privately. Referring to FIG. 3, a user at user computer 101 wishing to access Web pages 111 provided by Web server computer 103 preferably first downloads an anonymous access Web page 113 (this can be in the form of a button or label in one of the regular Web pages). This feature sends the request from user computer 101 to private portal server computer 107. Upon receiving the message, portal server 107 assigns a proxy identification to the user identification. Portal server 107 then forwards the message to Web server 103 using the proxy identification. Once the above links are established among user computer 101, portal server computer 107 and Web server computer 103, Web pages 111 can be browsed by the user anonymously. Further, more messages can be exchanged among them.

In addition, private portals of the present invention can be designed and created for a number of separate Web site providers who have a strategic alliance or business relationship with each other, each providing a common private entry point to their individual Web sites. For example, a "shopping mall" may provide a single private portal from which any of the e-merchants inside the "e-mall" may be accessed.

Referring to FIG. 4, identity bank 109 includes one or more databases. In particular, identity bank 109 includes a database 121 that stores true user identifications and a database 123 that stores proxy identifications. It should be noted that the proxy identification is constantly updated as discussed above. Further, the proxy identifications are generated by a random identification generator. The true user identifications are

assigned to the randomly generated proxy identifications by an ID router 125 which constantly updates the assignments. Alternatively, another trusted entity, other than the trusted third party maintaining private portal server 107, may actually hold the true user identifications and only provide an identification number or code to private portal server 107 to which a proxy identity is assigned. In this variation, identity bank 109 would hold only the proxy identifications and their corresponding identification codes, not the actual identification information, so that the trusted third party maintaining private portal server 107 assumes no liability for disclosing true user identifications.

By using the random identification generator a completely new proxy identity can be created upon each visit by any user. Alternatively, the randomly generated proxy identities are reused by different users. Thus, time correlated behavior information about a particular user is prevented. Note that in conventional systems when a proxy identity is purchased from some supplier for general use over the Internet, it is possible to track a specific user via their proxy identity over time.

Moreover, the present invention preferably does not require a user to purchase a proxy identity from any other party that he or she may then use at an arbitrary Web site. Upon visiting the private portal for any Web site, a user is automatically assigned a new proxy identity to use for as short a time as the user wishes. No purchase of proxy identities is needed. In addition, the Web site provider can tailor the user's private portal experience to suit his or her own business needs for the user experience they wish to provide.

However, in an alternative embodiment, a user may register a long-term proxy identity with the trusted third party so that the Web site may from time to time contact the anonymous user via a proxy email address assigned by the trusted third party.

It should be noted that the above described features of the trusted third party are preferably implemented in computer executable software programs. For instance, the features of generating proxy identities, forwarding and receiving messages to and from the user computer and the Web server, and mapping the true identities to the proxy identities are preferably implemented in computer executable programs.

The following examples discuss various embodiments of how the present invention can be utilized.

An investment banking or brokerage organization may provide a Web site where "research information" is provided to any user of the World Wide Web. Some parties who may be interested in that information are themselves large institutional investors whose market activities may be of particular interest to the brokerage organization providing the research information. The large institutional investor may be inhibited from accessing the brokerage Web site for fear of tipping off the brokerage firm on important stock market activities that may be performed by the institutional investor. It is therefore advantageous to the large institutional investor to remain anonymous from the brokerage Web site when it accesses research information. It is also advantageous for the brokerage firm to provide a private portal as access to its Web site so that its research information is readily available to any interested user who may otherwise be so distrustful as to ignore the Web site in the first place.

Another example teaches the value of the invention disclosed herein. Suppose an auction service (*e.g.*, Sotheby's) is provided online allowing user's to inspect items available for auction, and to submit bids anonymously. For example, if an auction house or other bidders became aware that the Metropolitan Museum of Modern Art was bidding on a particular art item, the price of the item could be bid up substantially, preventing the museum from participating in the first place.

Another example is a user who wishes to learn about tax case law in order to prepare his or her income tax filing for the Internal Revenue Service. A user may be hesitant to disclose any of his or her private information to the IRS while seeking information. In general, a private portal to a government Web site would provide for accessing public information from government sources without the threat of disclosing a citizen's true identity to that agency.

In still another example, a user who wishes to browse information on medical Web sites, such as information relating to medical devices and prescription medications, may not wish to disclose his or her identity to the entity maintaining the Web site. In addition, the recent Health Insurance Portability and Accountability Act of 1996 (HIPAA) lays out strict procedures for the protection of all individually identifiable health information that is or has been electronically transmitted. A private portal to a medical Web site would protect against the unauthorized collection and dissemination of a user's health-related information. Further, since HIPAA allows for the "reidentification" of

medical records and information in some cases, an identity map of user identities held by a trusted third party could be used to "reidentify" an individual user pursuant to HIPAA.

While the present invention has been described with reference to the preferred embodiments, those skilled in the art will recognize that numerous variations and modifications may be made without departing from the scope of the present invention. Accordingly, it should be clearly understood that the embodiments of the invention described above are not intended as limitations on the scope of the invention, which is defined only by the claims as allowed.

THE CLAIMS

What is claimed is:

1. A method of allowing a user at a first computer to communicate privately with a second computer, comprising:

receiving a request from the first computer to send a first message to the second computer, wherein the user has a first identification;

assigning a second identification to the user;

forwarding the first message to the second computer using the second identification;

receiving a second message from the second computer, wherein the second message includes customized information generated in response to the first message; and

forwarding the second message to the first computer using the first identification.

2. The method according to claim 1 wherein the step of assigning the second identification further comprises:

randomly generating a second identification.

3. The method according to claim 1 wherein the second message is an e-mail message.

4. The method according to claim 1 further comprising:

providing at least one of auction house services, brokerage firm services, investment banking services, governmental services and accounting firm services using the second computer.

5. The method according to claim 1 wherein the first message is written in a browser language.

6. The method according to claim 5 wherein the browser language is one of Hypertext Markup Language (HTML) and Extensible Markup Language (XML).

7. A system of allowing a user at a first computer to communicate privately with a second computer, comprising:

a server computer including:

a communication device configured to receive a request to send a first message to the second computer, wherein the user has a first identification; and

a processor configured to assign a second identification to the user, wherein the communication device is further configured to forward the first message to the second computer using the second identification, configured to receive a second message from the second computer and configured to forward the second message to the first computer using the first identification, wherein the second message includes customized information generated in response to the first message.

8. The system according to claim 7 the server further comprising:

an identification generator configured to generate randomly a plurality of second identifications.

9. The system according to claim 7 wherein the server is configured to provide at least one of auction house services, brokerage firm services, investment banking services, governmental services and accounting firm services using the second computer.

10. A software program implemented in a computer system for allowing a user at a first computer to communicate privately with a second computer, said software program configuring the computer system to:

receive a request from the first computer to send a first message to the second computer, wherein the user has a first identification;

assign a second identification to the user;

forward the first message to the second computer using the second identification;

receive a second message from the second computer, wherein the second message includes customized information generated in response to the first message; and

forward the second message to the first computer using the first identification.

11. The software according to claim 10 further configuring the computer system to:

randomly generate a second identification.

12. The software according to claim 11 wherein the second message is an e-mail message.

13. The software according to claim 10 further configuring the computer system to:

provide at least one of auction house services, brokerage firm services, investment banking services, governmental services and accounting firm services using the second computer.

14. The software according to claim 10 wherein the first message is written in a browser language.

15. The software according to claim 14 wherein the browser language is one of Hypertext Markup Language (HTML) and Extensible Markup Language (XML).

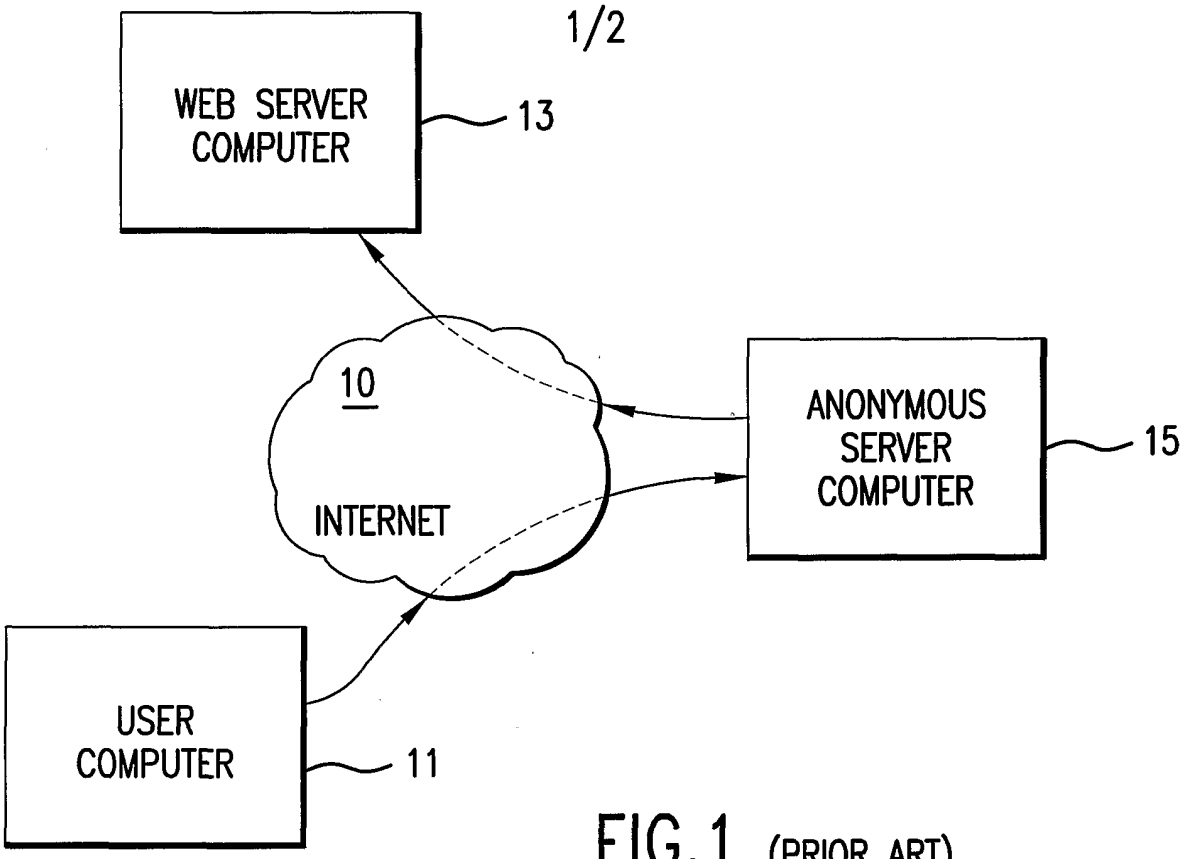


FIG.1 (PRIOR ART)

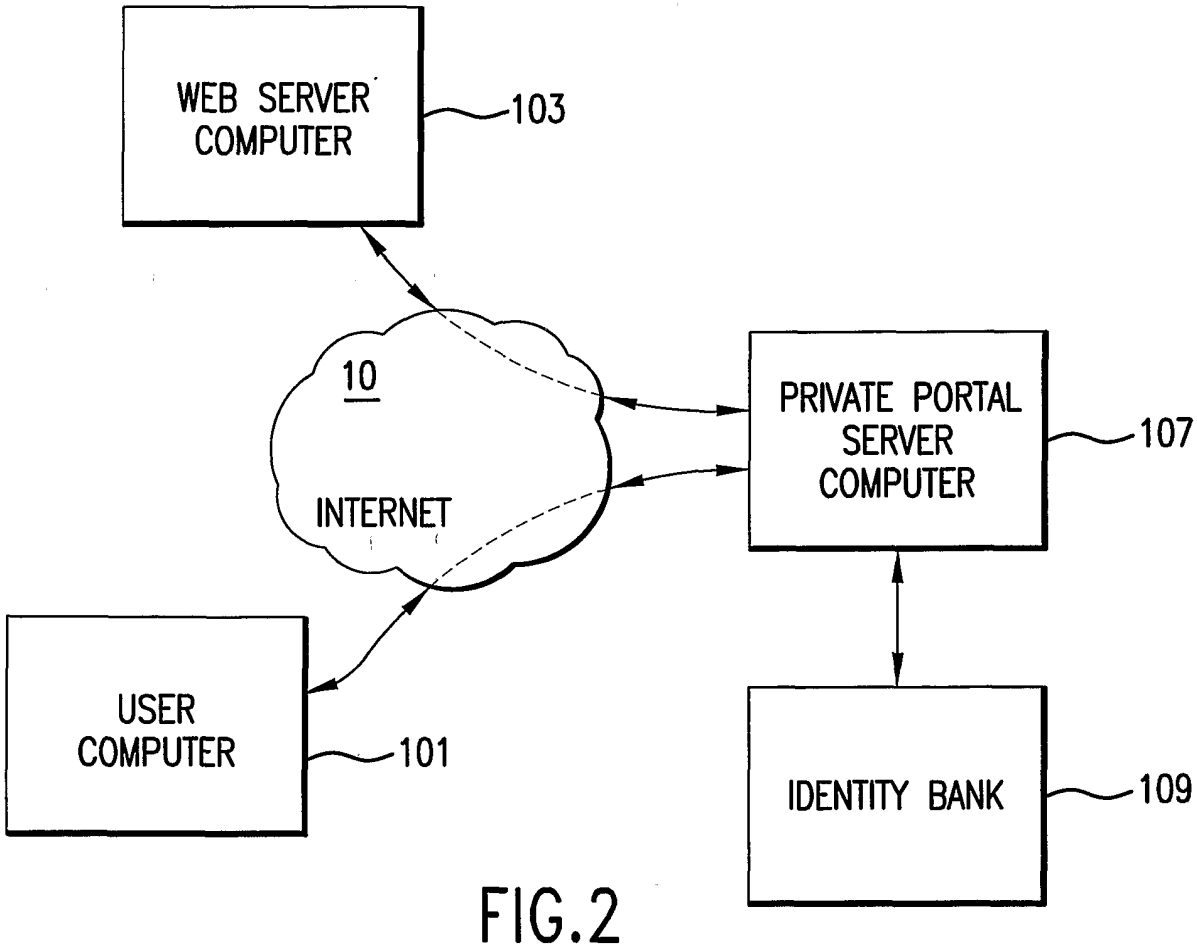


FIG.2

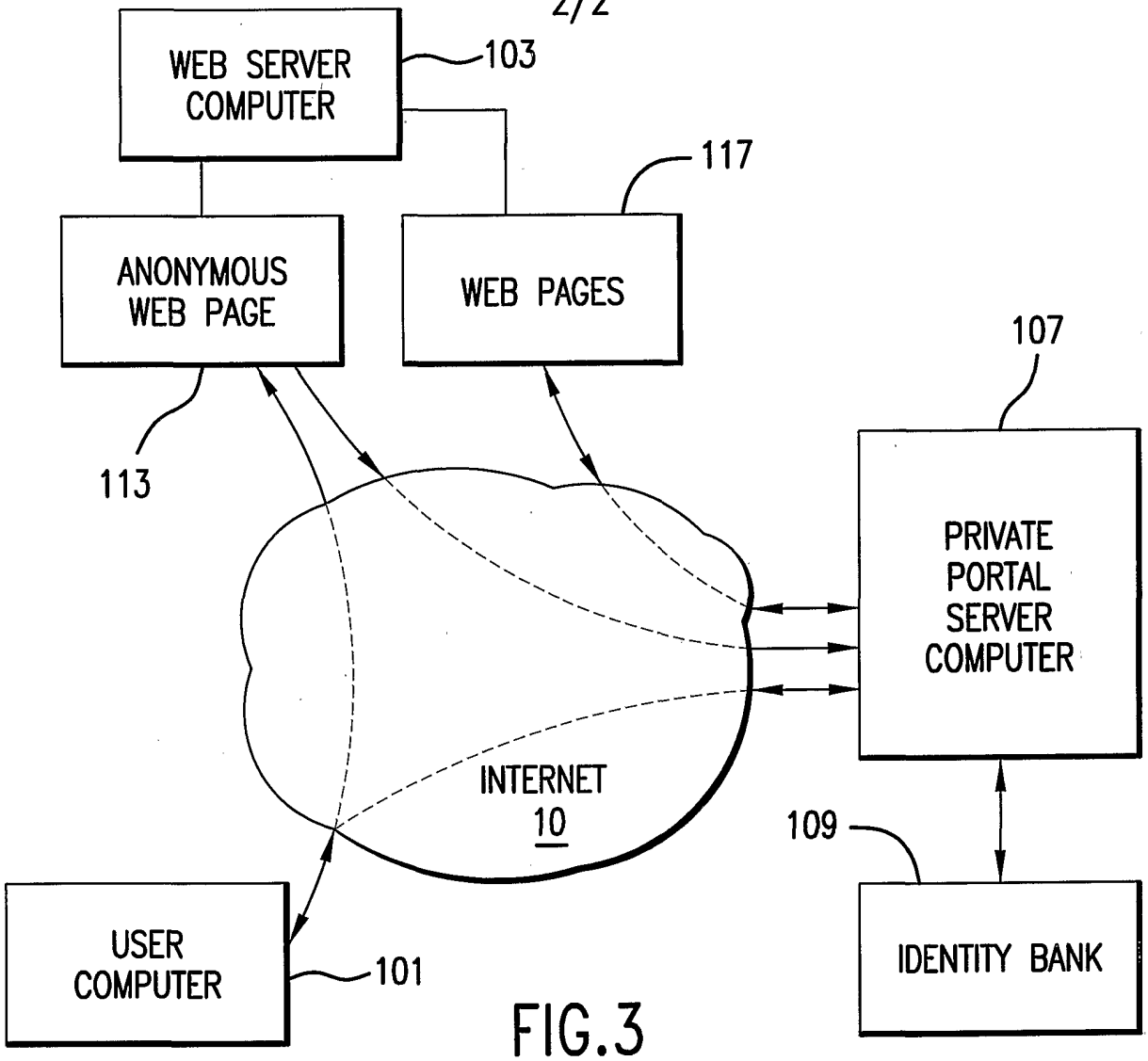

WEB SERVER COMPUTER
103
117
ANONYMOUS WEB PAGE
WEB PAGES
107
113
PRIVATE PORTAL SERVER COMPUTER
INTERNET
10
109
USER COMPUTER
101
IDENTITY BANK

FIG.3

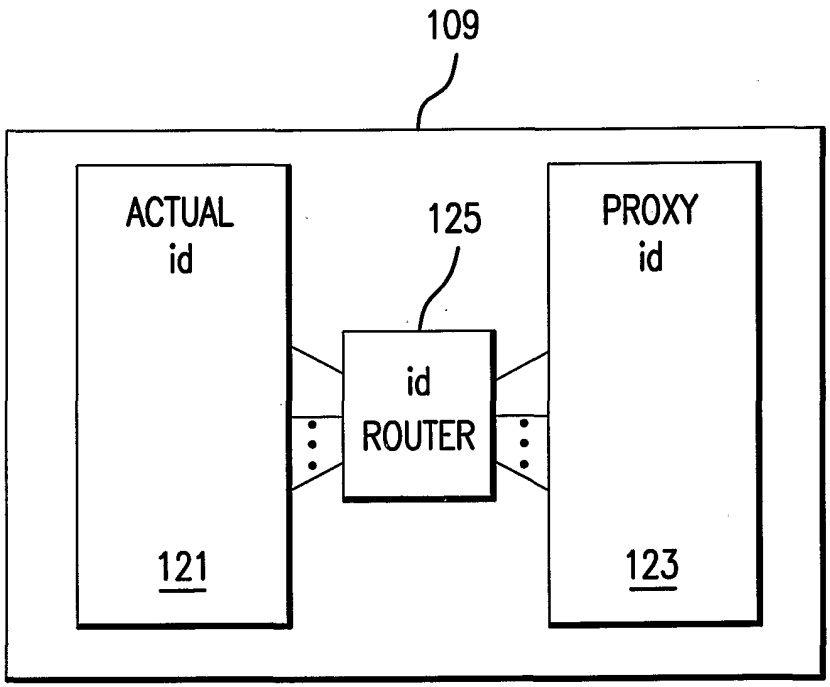

109
ACTUAL id
125
PROXY id
id ROUTER
121
123

FIG.4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/06143

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 13/00, 13/14, 15/16; G09C 3/00, H06F 1/26
US CL : 709/219, 228, 229, 206; 713/168, 201
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)

U.S. : 709/219, 228, 229, 206; 713/168, 201

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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,961,593 A (GABBER et al) 19 October 1999, abstract, col. 5, line 7- col. 15, line 7.	1-15
Y,P	US 6,148,343 A (LEWINE) 14 November 2000, in summary of the invention.	1-15
Y	US 5,907,667 A (GLENN et al) 25 May 1999, abstract, col. 3, line 66-col. 5, line 68.	1-15
Y,P	US 6,128,663 A (THOMAS) 03 October 2000, in summary of the invention.	1-15
Y,P	US 6,061,789 A (HAUSER et al) 09 May 2000, abstract, col. 4, line 7- col. 12, line 68	1-15

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"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
"A"	document defining the general state of the art which is not considered to be of particular relevance	"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
"E"	earlier document published on or after the international filing date	"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
"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)	"&"	document member of the same patent family
"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		

Date of the actual completion of the international search 13 APRIL 2001	Date of mailing of the international search report 22 MAY 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer GLENTON BURGESS Telephone No. (703) -305-4792

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/06143

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y,E	US 6,202,159 B1 (GHAFIR et al) 13 March 2001, abstract, col. 5, line 19- col. 9, line 58.	1-15.