

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
11 December 2003 (11.12.2003)

PCT

(10) International Publication Number
WO 03/102754 A1

(51) International Patent Classification⁷: G06F 7/00, 11/30, 12/14, 17/30, H04L 9/00

(74) Agent: DUNNING, Richard, A., Jr.; Law Office of Richard A. Dunning, Jr., 343 Soquel Avenue, Suite 311, Santa Cruz, CA 95062 (US).

(21) International Application Number: PCT/US03/16409

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, 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, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(22) International Filing Date: 23 May 2003 (23.05.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data: 10/159,532 31 May 2002 (31.05.2002) US

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

(71) Applicant (for all designated States except US): PLUMTREE SOFTWARE, INC. [US/US]; 500 Sansome Street, San Francisco, CA 94111 (US).

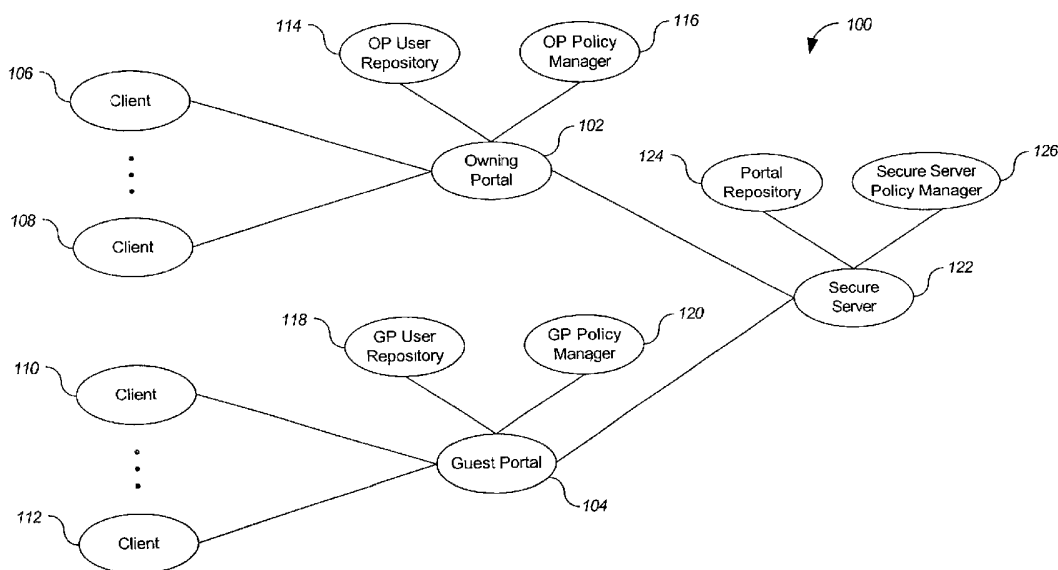
(72) Inventors; and

(75) Inventors/Applicants (for US only): FRIEDEN, Kurt [US/US]; 1562 San Lorenzo Ave., Berkeley, CA 94707 (US). RUDOMINER, Mitchell, B. [US/US]; 1752 Lexington Ave., El Cerrito, CA 94530 (US). MARKOFF, Matthew, S. [US/US]; 55 Oak Hill Road, Chappaqua, NY 10514 (US).

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: MANAGING SECURE RESOURCES IN WEB RESOURCES THAT ARE ACCESSED BY MULTIPLE PORTALS



(57) Abstract: A method, apparatus, and computer-readable media for authorizing users of network portals to access a secure resource hosted by a secure server (122) comprises storing a plurality of user identifiers (126), each representing a user of an owning portal; storing for each of the user identifiers an access privilege to the secure resource; storing a proxy user identifier representing a guest portal and a guest access privilege to the secure resource for all of the users of the guest portal.



WO 03/102754 A1

**Attorney Docket Number PLM024W01:
MANAGING SECURE RESOURCES IN WEB
RESOURCES THAT ARE ACCESSED BY MULTIPLE
PORTALS**

5

BACKGROUND

[0001] The present invention relates generally to data communication systems, and particularly to the use of network portals to access secure resources hosted by secure servers.

SUMMARY

[0002] In general, in one aspect, the invention features an apparatus for authorizing users of network portals to access a secure resource hosted by a secure server. It comprises an authorization table to store a plurality of user identifiers, each representing a user of an owning portal, and to store for each of the user identifiers an access privilege to the secure resource; wherein the authorization table stores a proxy user identifier representing a guest portal and a guest access privilege to the secure resource for all of the users of the guest portal; a policy manager to receive from the owning portal a first request for access to the secure resource, the first request comprising a first user identifier representing a user of the owning portal, wherein the policy manager grants to the user of the owning portal access to the secure resource according to the access privilege stored in the authorization table for the first user identifier; and wherein the policy manager receives from the guest portal a second request for access to the secure resource, the second request comprising a second user identifier representing a user of the guest portal and a portal identifier representing the guest portal, wherein the policy manager grants to the user of the guest portal access to the secure resource according to the guest access privilege stored in the authorization table for the proxy user identifier.

25

[0003] Particular implementations can include one or more of the following features. The first request comprises a portal identifier representing the owning portal, and implementations can comprise a portal repository to receive the first request, and to authenticate the owning portal using the portal identifier in the first request. Implementations

5 can comprise the owning portal, wherein the owning portal receives from the user of the owning portal a third request for access to the secure resource, the third request comprising the first user identifier and a security credential associated with the user of the owning portal; and a user repository to authenticate the user of the owning portal based on the first user identifier and the security credential associated with the user of the owning portal.

10 Implementations can comprise a portal policy manager to authorize the user of the owning portal based on the first user identifier; and the owning portal sends the first request to the secure server when the user of the owning portal is successfully authorized by the portal policy manager. Implementations can comprise a portal repository to receive the second request, and to authenticate the guest portal using the portal identifier in the second request.

15 Implementations can comprise the guest portal, wherein the guest portal receives from the user of the guest portal a fourth request for access to the secure resource, the fourth request comprising the second user identifier and a security credential associated with the user of the guest portal; and a user repository to authenticate the user of the guest portal based on the second user identifier and the security credential associated with the user of the guest portal.

20 Implementations can comprise a portal policy manager to authorize the user of the guest portal based on the second user identifier; and wherein the guest portal sends the second request to the secure server when the user of the guest portal is successfully authorized by the portal policy manager.

[0004] In general, in one aspect, the invention features a method, apparatus, and computer-readable media for authorizing users of network portals to access a secure resource hosted by a secure server. It comprises storing a plurality of user identifiers, each representing a user of an owning portal; storing for each of the user identifiers an access privilege to the secure resource; storing a proxy user identifier representing a guest portal and a guest access privilege to the secure resource for all of the users of the guest portal; receiving from the

25 owning portal a first request for access to the secure resource, the first request comprising a first user identifier representing a user of the owning portal; granting to the user of the

30

owning portal access to the secure resource according to the access privilege stored for the first user identifier; receiving from the guest portal a second request for access to the secure resource, the second request comprising a second user identifier representing a user of the guest portal and a portal identifier representing the guest portal; and granting to the user of the guest portal access to the secure resource according to the guest access privilege stored in the authorization table for the proxy user identifier.

[0005] Particular implementations can include one or more of the following features. The first request comprises a portal identifier representing the owning portal, and

implementations can comprise receiving the first request; and authenticating the owning

portal using the portal identifier in the first request. Implementations can comprise receiving at the owning portal from the user of the owning portal a third request for access to the secure resource, the third request comprising the first user identifier and a security credential associated with the user of the owning portal; and authenticating the user of the owning

portal based on the first user identifier and the security credential associated with the user of the owning portal. Implementations can comprise authorizing at the owning portal the user of

the owning portal based on the first user identifier; and sends the first request from the owning portal to the secure server when the user of the owning portal is successfully authorized. Implementations can comprise receiving the second request; and authenticating the guest portal using the portal identifier in the second request. Implementations can

comprise receiving at the guest portal from the user of the guest portal a fourth request for access to the secure resource, the fourth request comprising the second user identifier and a security credential associated with the user of the guest portal; and authenticating the user of the guest portal based on the second user identifier and the security credential associated with the user of the guest portal. Implementations can comprise authorizing at the guest portal the user of the guest portal based on the second user identifier; and sending the second request from the guest portal to the secure server when the user of the guest portal is successfully authorized by the portal policy manager.

[0006] The details of one or more implementations are set forth in the accompanying drawings and the description below. Other features will be apparent from the description and drawings, and from the claims.

DESCRIPTION OF DRAWINGS

[0007] FIG. 1 shows a communication system 100.

[0008] FIG. 2 shows an operation of the communication system of FIG. 1 in granting to a user of client access to a secure resource hosted by secure server according to one

5 implementation.

[0009] FIG. 3 shows an operation of the communication system of FIG. 1 in creating a project hosted by secure server according to one implementation.

[0010] FIG 4 shows an operation of the communication system of FIG. 1 in providing to users of a guest portal access to a secure resource according to one implementation.

10 [0011] The leading digit(s) of each reference numeral used in this specification indicates the number of the drawing in which the reference numeral first appears.

DETAILED DESCRIPTION

[0012] As used herein, the terms "client" and "server" generally refer to an electronic device or mechanism, and the term "message" generally refers to an electronic signal representing a digital message. As used herein, the term "mechanism" refers to hardware, software, or any
15 combination thereof. These terms are used to simplify the description that follows. The clients, servers, and mechanisms described herein can be implemented on any standard general-purpose computer, or can be implemented as specialized devices.

[0013] FIG. 1 shows a communication system 100. Communication system 100 includes an
20 owning portal 102 and a guest portal 104. Each portal serves one or more clients. Owning portal 102 serves a plurality of clients including clients 106 and 108. Guest portal 104 serves a plurality of clients including clients 110 and 112.

[0014] In the implementations discussed in detail herein, a user employs a client to send messages, such as requests for portal resources, to the portal that serves the client. In other
25 implementations, the clients operate automatically, without user intervention. Each portal authenticates its users using a user repository, and authorizes its clients to access portal resources using a portal policy manager. Referring again to FIG. 1, owning portal 102 uses a owning portal (OP) user repository 114 and an owning portal (OP) policy manager 116.

Guest portal 104 uses a guest portal (GP) user repository 118 and a guest portal (GP) policy
30 manager 120.

[0015] The user repositories 114, 118 are applications that authenticate users; that is, the user repositories verify the identity of users by comparing the authentication information supplied by the users to authentication information stored in the user repository. User authentication information generally includes a user identifier and a security credential for each user. In
5 some implementations, the portals 102, 104 authenticate the users with http basic authentication, the user identifier is a userid, and the security credential is a password. User repositories 114, 118 can be hosted by portals 102, 104, or can be externally-provided applications, such as lightweight directory access protocol (LDAP) services.

[0016] The portal policy managers 116, 120 are applications that authorize users to perform
10 certain tasks, such as to access secure information or resources, according to roles and privileges assigned to the users. Each portal policy manager authorizes the clients served by its portal to access portal resources that are provided by the portal. These resources can include providing information to the user and the like. Some of the resources provided by the portal are hosted by other servers. Referring again to FIG. 1, some of the resources provided
15 by portal 102 are secure resources hosted by a secure server 122. A secure resource is a resource that requires the user be authorized to access the secure resource.

[0017] One type of secure resource is a project. A project can be created only by a user of the owning portal having the role of community manager, as described below. OP policy manager 116 stores the user identifiers of the community managers that are allowed to create
20 projects on secure server 122. A project acts as a container for other types of secure resources, such as events, milestones, discussions, documents, folders, and the like. Secure resource policy manager 126 stores the user identifiers of the users that are allowed to access the secure resources hosted by secure server 122. For each secure resource hosted by secure server 122, secure server policy manager 126 stores the users allowed to access the secure
25 resource, and the access privileges of each user for that secure resource. In one implementation, access privileges are defined by roles. Each role for a secure resource has an access level and activity security. For example, in a discussion, a user having a role with the highest access level, allowing him to change the name and description of the discussion, and to edit its security policy, while users having a role with a lower access level cannot. Activity
30 security settings allow certain users to start new threads and to reply to messages in the discussion.

[0018] FIG. 2 shows an operation 200 of communication system 100 in granting to a user of client 106 access to a secure resource hosted by secure server 122 according to one implementation. A user operates client 106 to request the secure resource (step 202). Client 106 sends to portal 102 a message requesting access to the secure resource (step 204). The message includes user authentication information, such as a http basic authentication header including a userid and password for the user, a cookie issued by portal 102 after a previous successful authentication, or the like. User repository 114 attempts to authenticate the user (step 206).

[0019] After a successful authentication, policy manager 116 examines the request to determine whether the user must be authorized by portal 102. Requests to access secure resources provided by portal 102 require authorization by portal 102. Therefore portal 102 attempts to authorize the user to communicate with secure server 122 (step 208). Policy managers 116 and 120 store the user identifiers of the users that are allowed to communicate with secure server 122. Policy manager 116 determines whether the user is authorized to communicate with secure server 122. If the authorization fails, portal 102 informs the user.

[0020] After a successful authorization, portal 102 then sends the request, and portal authentication information, to secure server 122 (step 210). The portal authentication information includes authentication information for the portal such as a http basic authentication header including a portal identifier and password for the portal, a cookie issued by secure server 122 after a previous successful authentication, or the like. A portal repository 124 attempts to authenticate the portal by comparing the authentication information to information stored in portal repository 124 (step 212). After a successful authentication of portal 102, portal repository 124 trusts portal 102, and so does not attempt to authenticate the user.

[0021] After a successful authentication of portal 102, secure server policy manager 126 attempts to authorize the user to access the requested secure resource; that is, policy manager 126 determines whether the user is authorized to access the secure resource requested by the user (step 214). For each secure resource hosted by secure server 122, policy manager 126 includes an authorization table that stores the user identifiers of the users of portal 102 that are authorized to access the secure resource, the role of each user, and the privileges associated with that role. In some implementations, the roles include leader, member and

guest, and the privileges include read access and write access. After a successful authorization, secure server 122 grants access to the secure resource to the user according to the user's privileges (step 216).

[0022] Certain users of portal 102 can create projects upon secure server 122. Portal policy manager 116 defines roles and privileges for each user served by portal 102. One of the roles is community manager. A community manager has the privilege of creating projects.

[0023] FIG. 3 shows an operation 300 of communication system 100 in creating a project hosted by secure server 122 according to one implementation. A user having the role of community manager (referred to hereinafter simply as "the community manager") operates client 108 to request the creation of a project (step 302). Client 108 therefore sends to portal 102 a message requesting the creation of a project (step 304). The message includes user authentication information. User repository 114 attempts to authenticate the community manager by comparing the authentication information to information stored in user repository 114 (step 306).

[0024] After a successful authentication, policy manager 116 examines the request to determine whether the community manager must be authorized. Requests to create a project require authorization by portal 102. Therefore policy manager 116 attempts to authorize the community manager by comparing the community manager's identity to information stored by policy manager 116 (step 308). Policy manager 116 determines that the community manager has the role of community manager, and therefore the community manager has the privilege of creating projects. Therefore policy manager 116 authorizes the community manager.

[0025] After a successful authorization, portal 102 then sends the request, and portal authentication information, to secure server 122 (step 310). Because the user is a community manager, portal 102 includes a role identifier in the request that identifies the user as a community manager. Portal repository 124 attempts to authenticate the portal by comparing the authentication information to information stored in portal repository 124 (step 312). After a successful authentication of portal 102, portal repository 124 trusts portal 102, and so does not attempt to authenticate the community manager. The secure server also trusts the role identifier provided by portal 102, and so permits the community manager to create a new project.

[0026] The community manager then creates the project (step 314). After a community manager creates a project, he selects the users he wishes to access that project, and assigns a role to each of those users. Secure server policy manager 126 then stores, for the project, the identities of the users that can access the project, the role of each user for that project, and the privileges assigned to each role. This information is stored in an authorization table for the project.

[0027] In general, secure server 122 and the secure resources hosted thereon are established by the administrator of the owning portal. In other words, the owning portal "owns" secure server 122 and the secure resources hosted thereon. At times it is desirable to allow users of other portals, referred to herein as "guest portals" to access the secured resources owned by the owning portal. For example, a car company Carco has established owning portal 102 and a secure server 122, and has established a secure resource on the secure server in the form of a production schedule. A parts company Partco supplies car parts to Carco. In order to streamline operations, Carco would like to give Partco limited access to the production schedule.

[0028] FIG 4 shows an operation 400 of communication system 100 in providing to users of a guest portal access to a secure resource according to one implementation. An administrator of owning portal 102 assigns a proxy user identifier to guest portal 104 (step 402). The proxy user identifier represents all of the users of guest portal 104. The administrator then associates a role with the proxy user identifier (step 404). The role conveys certain access privileges to the secure resource. Therefore, all of the users of guest portal 104 have the same access privileges to the secure resource. The proxy user identifier is associated with a portal identifier of guest portal 104. The proxy user identifier, portal identifier and role for guest portal 104 are stored in an authorization table within secure server policy manager 126. The portal identifier and a security credential for guest portal 104 are stored in portal repository 124.

[0029] A user of one of the clients served by guest portal 104, say client 110, generates a request to access a secure resource hosted by secure server 122 (step 406). Client 110 sends to guest portal 104 a message requesting access to the secure resource (step 408). Guest portal 104 receives the request, and attempts to authenticate the user in a manner similar to that described for owning portal 102 (step 410). After a successful authentication, guest

portal 104 attempts to authorize the user in a manner similar to that described for owning portal 102 (step 412). After a successful authorization, guest portal 104 passes the request to secure server 122 (step 414). Portal repository 124 attempts to authenticate the portal, as described above for owning portal 102 (step 416). After a successful authentication, policy manager 126 attempts to authorize the user (step 418).

[0030] The request includes a portal identifier for guest portal 104. Policy manager 126 uses the portal identifier in the request to locate the role for the guest portal in the authorization table. If the portal identifier cannot be found, the user is not authorized, and the request for access is denied. However, if the portal identifier is found, access is granted to the user in accordance with the privileges of the role assigned to the proxy user identifier associated with the portal identifier (step 420).

[0031] The techniques describe herein permit an enterprise network administrator to grant to other parties limited access to secured enterprise resources without requiring those other parties to expose their user repositories to the enterprise. Returning to the Carco/Partco example, although Partco would like to view the production Carco schedule, Partco may not wish to disclose all of the employee information contained in its user repository.

[0032] These techniques also permit an enterprise network administrator to easily provide limited access to other parties. The administrator need not deal with another user repository, but need only deal with large collections of users represented by guest portals, and can assign the same access privileges to all of those users quickly and easily. For example, Carco may wish Partco to view its production schedule, but probably would not allow Partco to modify the schedule.

[0033] The invention can be implemented in digital electronic circuitry, or in computer hardware, firmware, software, or in combinations of them. Apparatus of the invention can be implemented in a computer program product tangibly embodied in a machine-readable storage device for execution by a programmable processor; and method steps of the invention can be performed by a programmable processor executing a program of instructions to perform functions of the invention by operating on input data and generating output. The invention can be implemented advantageously in one or more computer programs that are executable on a programmable system including at least one programmable processor coupled to receive data and instructions from, and to transmit data and instructions to, a data

storage system, at least one input device, and at least one output device. Each computer program can be implemented in a high-level procedural or object-oriented programming language, or in assembly or machine language if desired; and in any case, the language can be a compiled or interpreted language. Suitable processors include, by way of example, both
5 general and special purpose microprocessors. Generally, a processor will receive instructions and data from a read-only memory and/or a random access memory. Generally, a computer will include one or more mass storage devices for storing data files; such devices include magnetic disks, such as internal hard disks and removable disks; magneto-optical disks; and optical disks. Storage devices suitable for tangibly embodying computer program instructions
10 and data include all forms of non-volatile memory, including by way of example semiconductor memory devices, such as EPROM, EEPROM, and flash memory devices; magnetic disks such as internal hard disks and removable disks; magneto-optical disks; and CD-ROM disks. Any of the foregoing can be supplemented by, or incorporated in, ASICs (application-specific integrated circuits) .

15 [0034] A number of implementations of the invention have been described. Nevertheless, it will be understood that various modifications may be made without departing from the spirit and scope of the invention. Accordingly, other implementations are within the scope of the following claims.

WHAT IS CLAIMED IS:

- 3 1. An apparatus for authorizing users of network portals to access a secure resource hosted by a secure server, comprising:
- an authorization table to store a plurality of user identifiers, each representing a user of an owning portal, and to store for each of the user identifiers an access privilege to the secure resource;
 - 5 wherein the authorization table stores a proxy user identifier representing a guest portal and a guest access privilege to the secure resource for all of the users of the guest portal;
 - a policy manager to receive from the owning portal a first request for access to the secure resource, the first request comprising a first user identifier representing a user of the
0 owning portal, wherein the policy manager grants to the user of the owning portal access to

the secure resource according to the access privilege stored in the authorization table for the first user identifier; and

wherein the policy manager receives from the guest portal a second request for access to the secure resource, the second request comprising a second user identifier representing a user of the guest portal and a portal identifier representing the guest portal, wherein the policy manager grants to the user of the guest portal access to the secure resource according to the guest access privilege stored in the authorization table for the proxy user identifier.

2. The apparatus of claim 1, wherein the first request comprises a portal identifier representing the owning portal, further comprising:

a portal repository to receive the first request, and to authenticate the owning portal using the portal identifier in the first request.

3. The apparatus of claim 1, further comprising:

the owning portal, wherein the owning portal receives from the user of the owning portal a third request for access to the secure resource, the third request comprising the first user identifier and a security credential associated with the user of the owning portal; and

a user repository to authenticate the user of the owning portal based on the first user identifier and the security credential associated with the user of the owning portal.

4. The apparatus of claim 3, further comprising:

a portal policy manager to authorize the user of the owning portal based on the first user identifier; and

wherein the owning portal sends the first request to the secure server when the user of the owning portal is successfully authorized by the portal policy manager.

5. The apparatus of claim 1, further comprising:

a portal repository to receive the second request, and to authenticate the guest portal using the portal identifier in the second request.

6. The apparatus of claim 1, further comprising:

the guest portal, wherein the guest portal receives from the user of the guest portal a fourth request for access to the secure resource, the fourth request comprising the second user identifier and a security credential associated with the user of the guest portal; and

a user repository to authenticate the user of the guest portal based on the second user identifier and the security credential associated with the user of the guest portal.

7. The apparatus of claim 6, further comprising:

a portal policy manager to authorize the user of the guest portal based on the second user identifier; and

wherein the guest portal sends the second request to the secure server when the user of the guest portal is successfully authorized by the portal policy manager.

8. An apparatus for authorizing users of network portals to access a secure resource hosted by a secure server, comprising:

means for storing a plurality of user identifiers, each representing a user of an owning portal, and to store for each of the user identifiers an access privilege to the secure resource;

wherein the means for storing stores a proxy user identifier representing a guest portal and a guest access privilege to the secure resource for all of the users of the guest portal;

policy manager means for receiving from the owning portal a first request for access to the secure resource, the first request comprising a first user identifier representing a user of the owning portal, wherein the policy manager grants to the user of the owning portal access to the secure resource according to the access privilege stored in the authorization table for the first user identifier; and

wherein the policy manager means receives from the guest portal a second request for access to the secure resource, the second request comprising a second user identifier representing a user of the guest portal and a portal identifier representing the guest portal, wherein the policy manager grants to the user of the guest portal access to the secure resource according to the guest access privilege stored in the authorization table for the proxy user identifier.

9. The apparatus of claim 8, wherein the first request comprises a portal identifier representing the owning portal, further comprising:

portal repository means for receiving the first request, and for authenticating the owning portal using the portal identifier in the first request.

5

10. The apparatus of claim 8, further comprising:

the owning portal, wherein the owning portal receives from the user of the owning portal a third request for access to the secure resource, the third request comprising the first user identifier and a security credential associated with the user of the owning portal; and

0

user repository means for authenticating the user of the owning portal based on the first user identifier and the security credential associated with the user of the owning portal.

11. The apparatus of claim 10, further comprising:

portal policy manager means for authorizing the user of the owning portal based on the first user identifier; and

5

wherein the owning portal sends the first request to the secure server when the user of the owning portal is successfully authorized by the portal policy manager.

12. The apparatus of claim 8, further comprising:

portal repository means for receiving the second request, and for authenticating the guest portal using the portal identifier in the second request.

0

13. The apparatus of claim 8, further comprising:

the guest portal, wherein the guest portal receives from the user of the guest portal a fourth request for access to the secure resource, the fourth request comprising the second user identifier and a security credential associated with the user of the guest portal; and

5

user repository means for authenticating the user of the guest portal based on the second user identifier and the security credential associated with the user of the guest portal.

10

14. The apparatus of claim 13, further comprising:

portal policy manager means for authorizing the user of the guest portal based on the second user identifier; and

wherein the guest portal sends the second request to the secure server when the user of the guest portal is successfully authorized by the portal policy manager.

5

15. A method for authorizing users of network portals to access a secure resource hosted by a secure server, comprising:

storing a plurality of user identifiers, each representing a user of an owning portal;

storing for each of the user identifiers an access privilege to the secure resource;

0

storing a proxy user identifier representing a guest portal and a guest access privilege to the secure resource for all of the users of the guest portal;

receiving from the owning portal a first request for access to the secure resource, the first request comprising a first user identifier representing a user of the owning portal;

5

granting to the user of the owning portal access to the secure resource according to the access privilege stored for the first user identifier;

receiving from the guest portal a second request for access to the secure resource, the second request comprising a second user identifier representing a user of the guest portal and a portal identifier representing the guest portal; and

0

granting to the user of the guest portal access to the secure resource according to the guest access privilege stored in the authorization table for the proxy user identifier.

16. The method of claim 15, wherein the first request comprises a portal identifier representing the owning portal, further comprising:

receiving the first request; and

5

authenticating the owning portal using the portal identifier in the first request.

17. The method of claim 15, further comprising:

receiving at the owning portal from the user of the owning portal a third request for access to the secure resource, the third request comprising the first user identifier and a security credential associated with the user of the owning portal; and

10

authenticating the user of the owning portal based on the first user identifier and the security credential associated with the user of the owning portal.

18. The method of claim 17, further comprising:

authorizing at the owning portal the user of the owning portal based on the first user identifier; and

sending the first request from the owning portal to the secure server when the user of the owning portal is successfully authorized.

19. The method of claim 15, further comprising:

receiving the second request; and

authenticating the guest portal using the portal identifier in the second request.

20. The method of claim 15, further comprising:

receiving at the guest portal from the user of the guest portal a fourth request for access to the secure resource, the fourth request comprising the second user identifier and a security credential associated with the user of the guest portal; and

authenticating the user of the guest portal based on the second user identifier and the security credential associated with the user of the guest portal.

21. The method of claim 20, further comprising:

authorizing at the guest portal the user of the guest portal based on the second user identifier; and

sending the second request from the guest portal to the secure server when the user of the guest portal is successfully authorized by the portal policy manager.

22. Computer-readable media embodying instructions executable by a computer to perform a method for authorizing users of network portals to access a secure resource hosted by a secure server, the method comprising:

storing a plurality of user identifiers, each representing a user of an owning portal;

storing for each of the user identifiers an access privilege to the secure resource;

storing a proxy user identifier representing a guest portal and a guest access privilege to the secure resource for all of the users of the guest portal;

receiving from the owning portal a first request for access to the secure resource, the first request comprising a first user identifier representing a user of the owning portal

granting to the user of the owning portal access to the secure resource according to the access privilege stored for the first user identifier;

receiving from the guest portal a second request for access to the secure resource, the second request comprising a second user identifier representing a user of the guest portal and a portal identifier representing the guest portal; and

granting to the user of the guest portal access to the secure resource according to the guest access privilege stored in the authorization table for the proxy user identifier.

23. The media of claim 22, wherein the first request comprises a portal identifier representing the owning portal, wherein the method further comprises:

receiving the first request; and

authenticating the owning portal using the portal identifier in the first request.

24. The media of claim 22, wherein the method further comprises:

receiving at the owning portal from the user of the owning portal a third request for access to the secure resource, the third request comprising the first user identifier and a security credential associated with the user of the owning portal; and

authenticating the user of the owning portal based on the first user identifier and the security credential associated with the user of the owning portal.

25. The media of claim 24, wherein the method further comprises:

authorizing at the owning portal the user of the owning portal based on the first user identifier; and

sends the first request from the owning portal to the secure server when the user of the owning portal is successfully authorized.

26. The media of claim 22, wherein the method further comprises:

receiving the second request; and
authenticating the guest portal using the portal identifier in the second request.

27. The media of claim 22, wherein the method further comprises:

5 receiving at the guest portal from the user of the guest portal a fourth request for access to the secure resource, the fourth request comprising the second user identifier and a security credential associated with the user of the guest portal; and

authenticating the user of the guest portal based on the second user identifier and the security credential associated with the user of the guest portal.

) 28. The media of claim 27, wherein the method further comprises:

authorizing at the guest portal the user of the guest portal based on the second user identifier; and

5 sending the second request from the guest portal to the secure server when the user of the guest portal is successfully authorized by the portal policy manager.

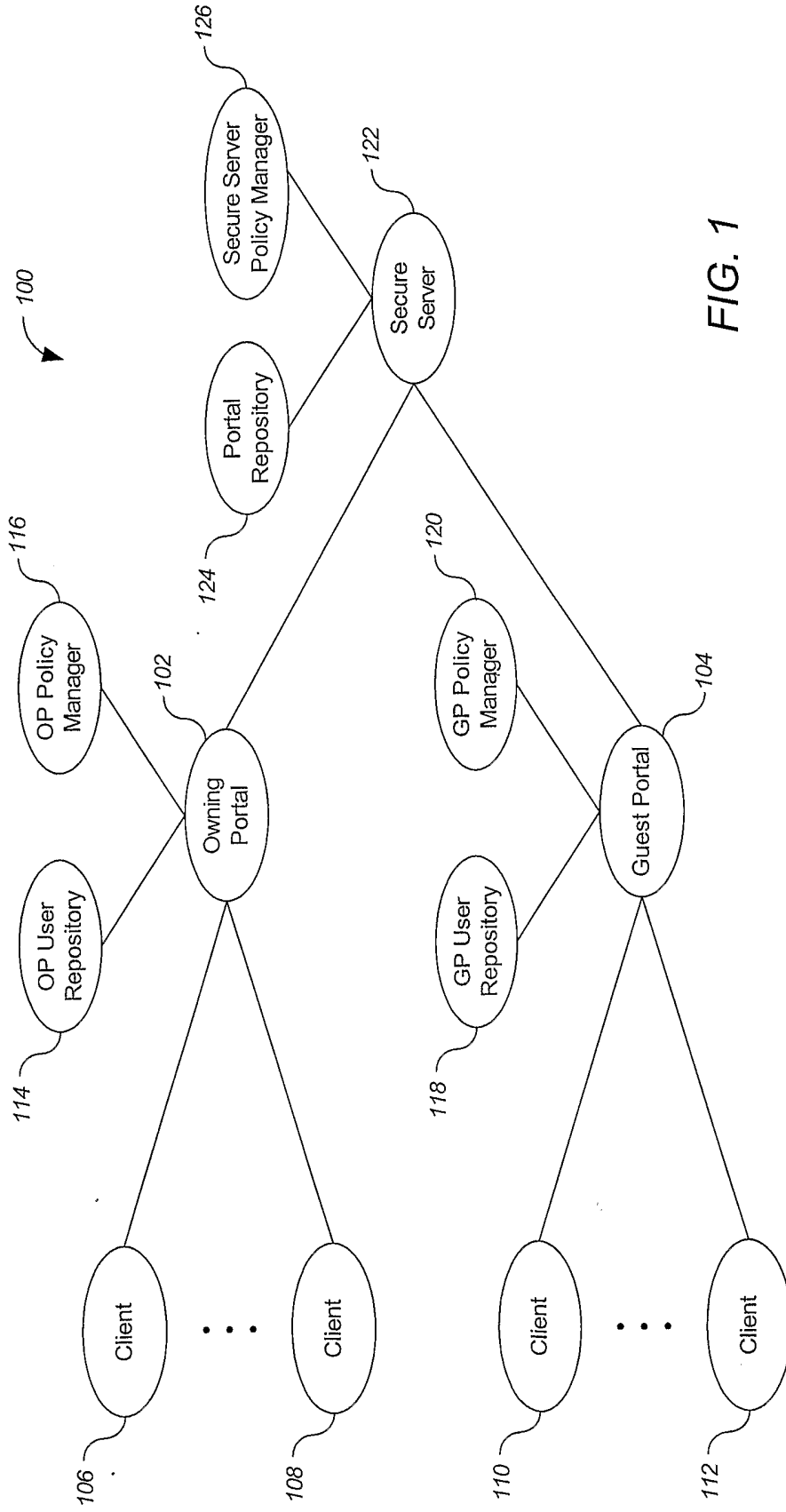


FIG. 1

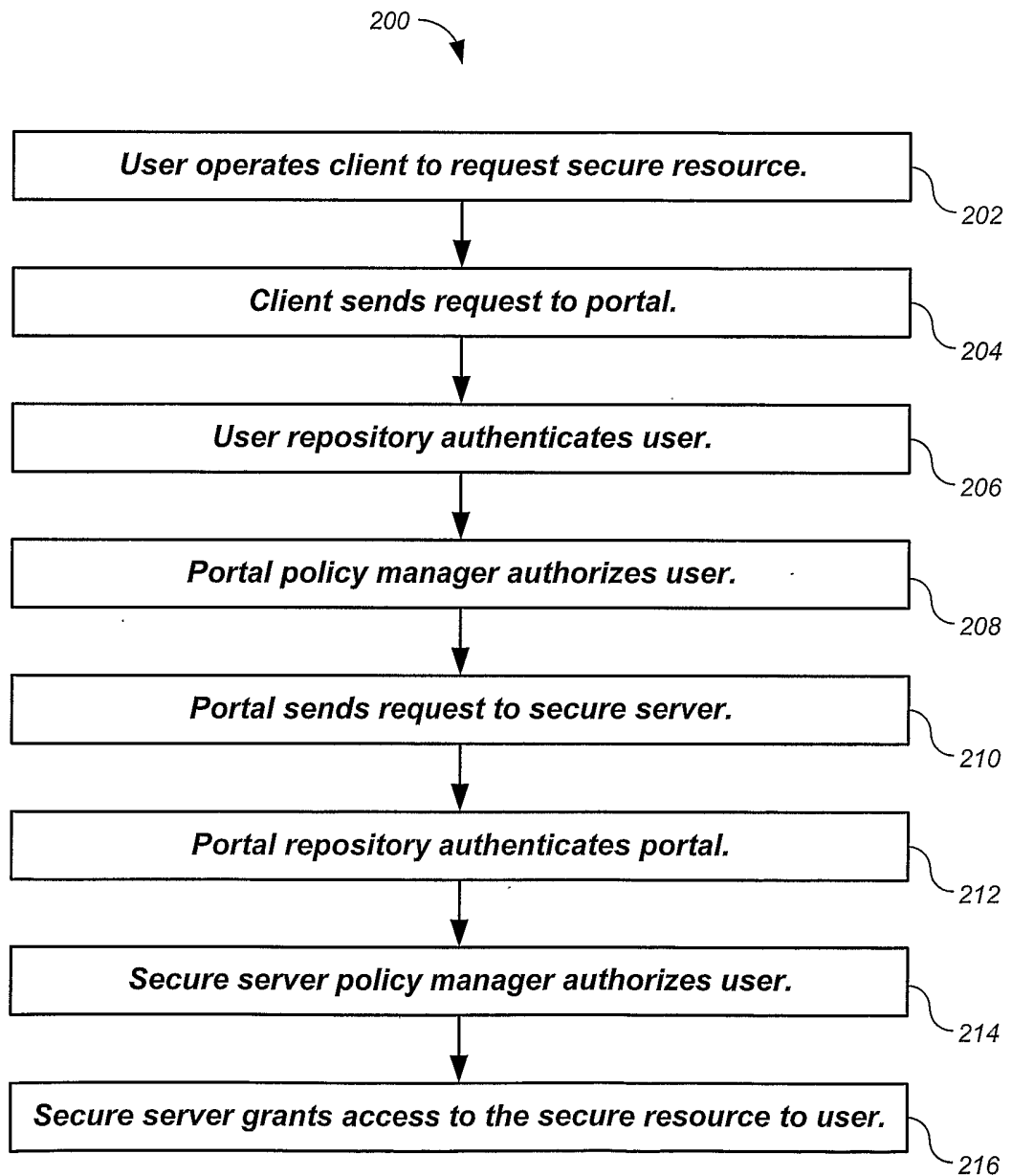


FIG. 2

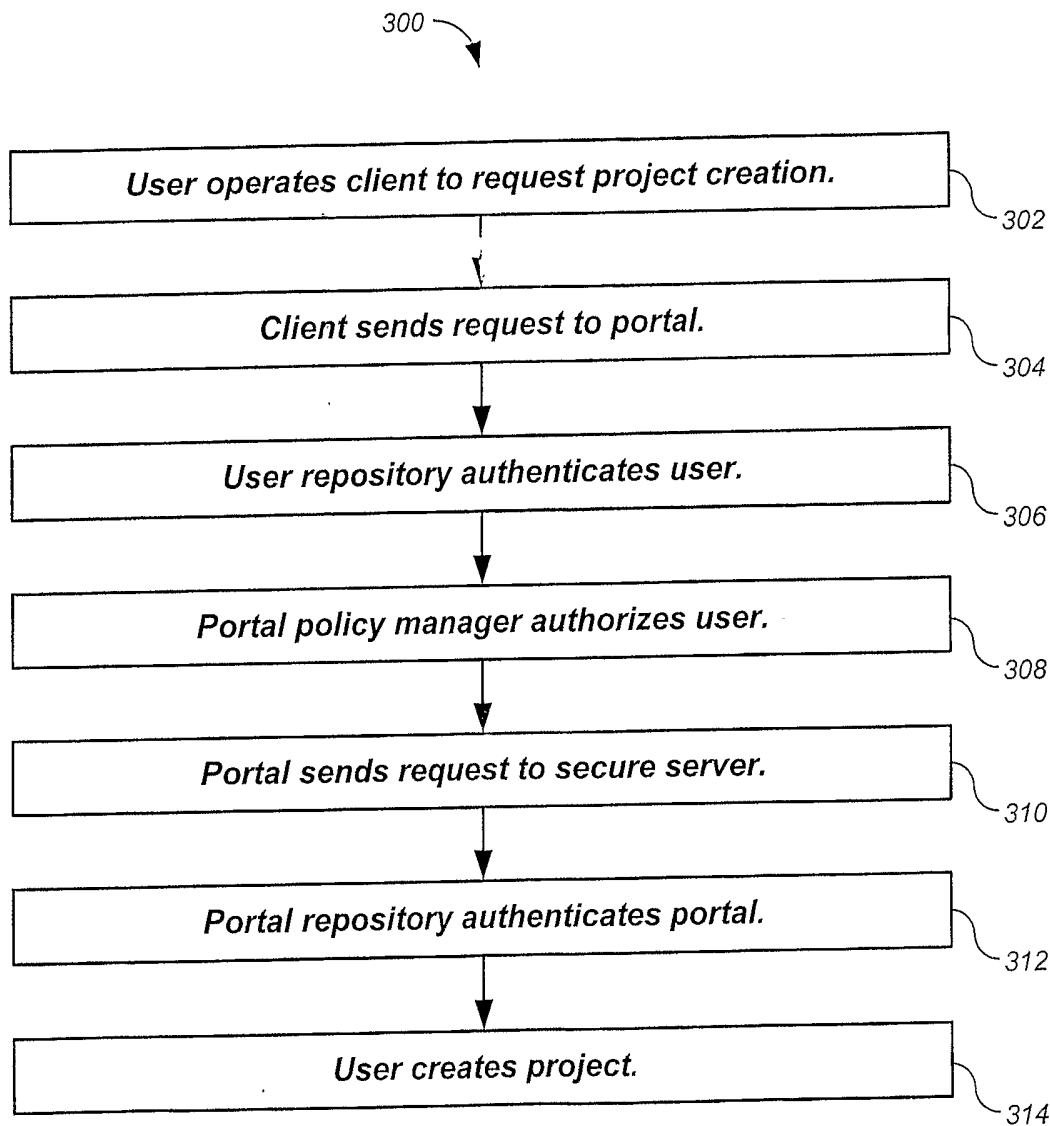


FIG. 3

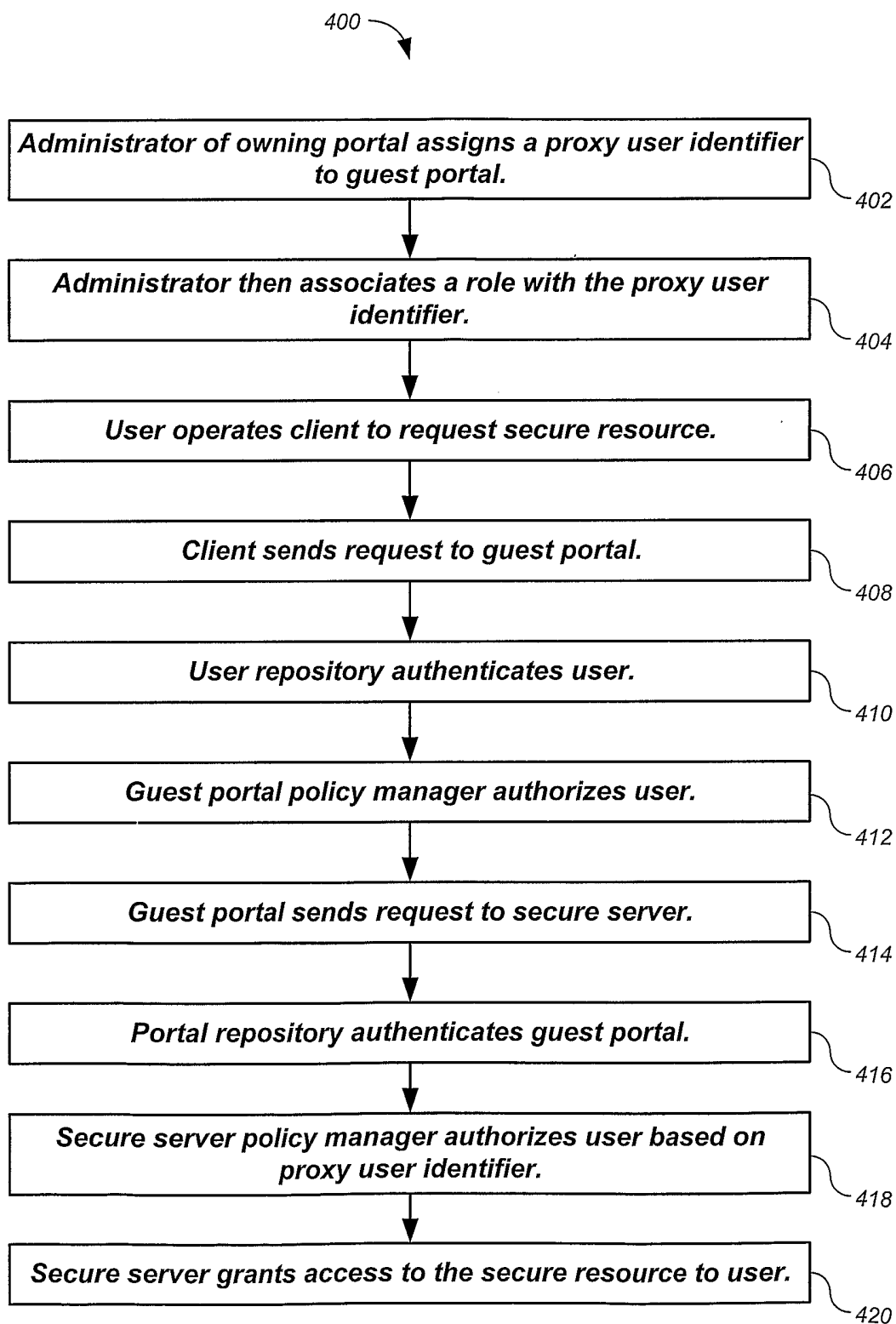


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US03/16409

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 7/00, 11/30, 12/14, 17/30; H04L 9/00
 US CL : 707/9; 713/181, 200, 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. : 707/9; 713/181, 200, 201, 202

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 6,088,451 A (He et al.) 11 July 2000 (11.07.2000), column 1, line 1 - column 33, line 67.	1-28
Y	US 6,249,873 B1 (Richard et al.) 19 June 2001 (19.06.2001), column 1, line 1 - column 12, line 67.	1-28
Y	US 5,970,143 A (Schneier et al.) 19 October 1999 (19.10.1999), column 1, line 1 - column 76, line 67.	1-28

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	"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
"E"	earlier application or patent published on or after the international filing date	"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
"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)	"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
"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	"&" document member of the same patent family

Date of the actual completion of the international search

11 August 2003 (11.08.2003)

Date of mailing of the international search report

27 AUG 2003

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US
 Commissioner for Patents
 P.O. Box 1450
 Alexandria, Virginia 22313-1450

Facsimile No. (703)305-3230

Authorized officer

Chongshan Chen *James R. Matthews*
 Telephone No. (703)305-3900