US 20030115292A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2003/0115292 A1

Griffin et al. (43) Pub. Date: Jun. 19, 2003

(54) SYSTEM AND METHOD FOR DELEGATED ADMINISTRATION

(76) Inventors: **Philip B. Griffin**, Longmont, CO (US); **Manish Devgan**, Bloomfield, CO (US); **Christopher E. Bales**, Boulder, CO (US); **Chris Fregly**, Hoffman Estates, IL (US); **Dmitry Dimov**, San Francisco, CA (US)

Correspondence Address:
FLIESLER DUBB MEYER & LOVEJOY, LLP
FOUR EMBARCADERO CENTER
SUITE 400
SAN FRANCISCO, CA 94111 (US)

(21) Appl. No.: **10/279,543**

(22) Filed: **Oct. 24, 2002**

Related U.S. Application Data

(60) Provisional application No. 60/386,487, filed on Oct. 24, 2001.

Publication Classification

(51) **Int. Cl.**[7] **G06F 15/16**

(52) **U.S. Cl.** **709/219**

(57) **ABSTRACT**

A system and method for delegating administration tasks comprising determining at least one capability for a first user based on evaluation of at least one role rule and delegating the at least one capability to a second user.

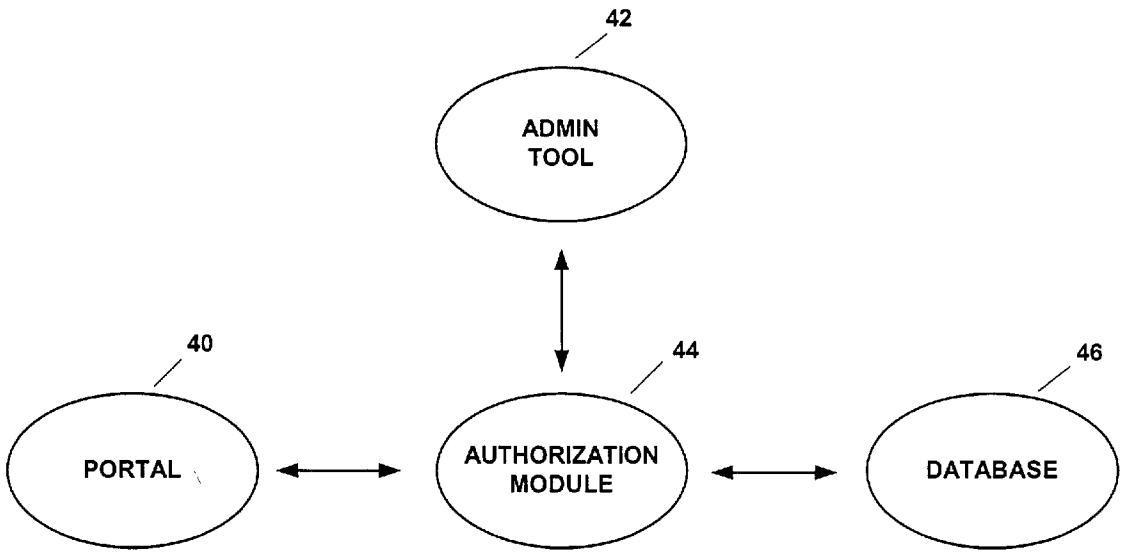


FIG. 1

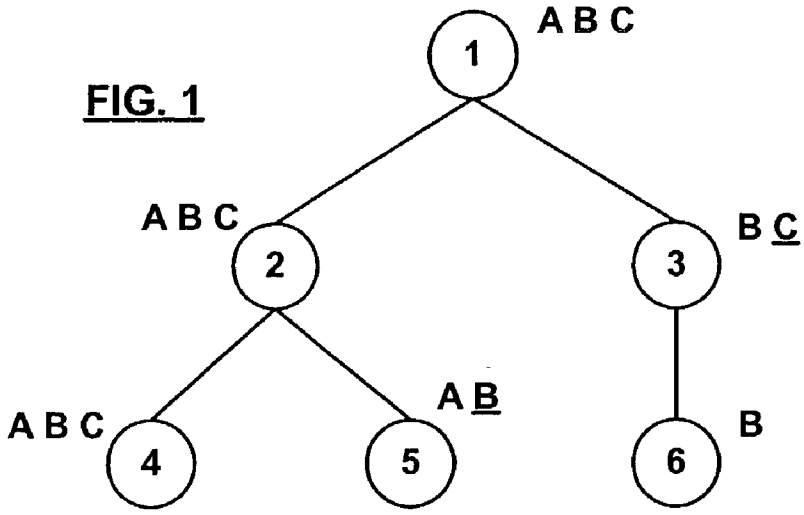
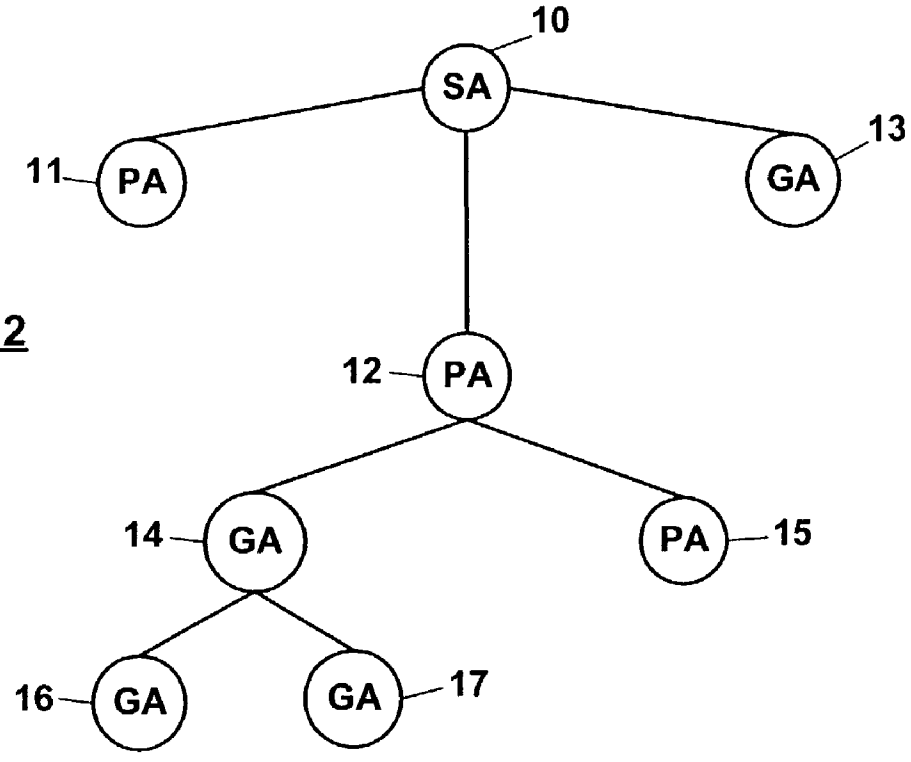

A B C
1
A B C
2
B C
3
A B C
4
A B
5
B
6

FIG. 2


10
SA
11
PA
13
GA
12
PA
14
GA
PA
15
16
GA
GA
17

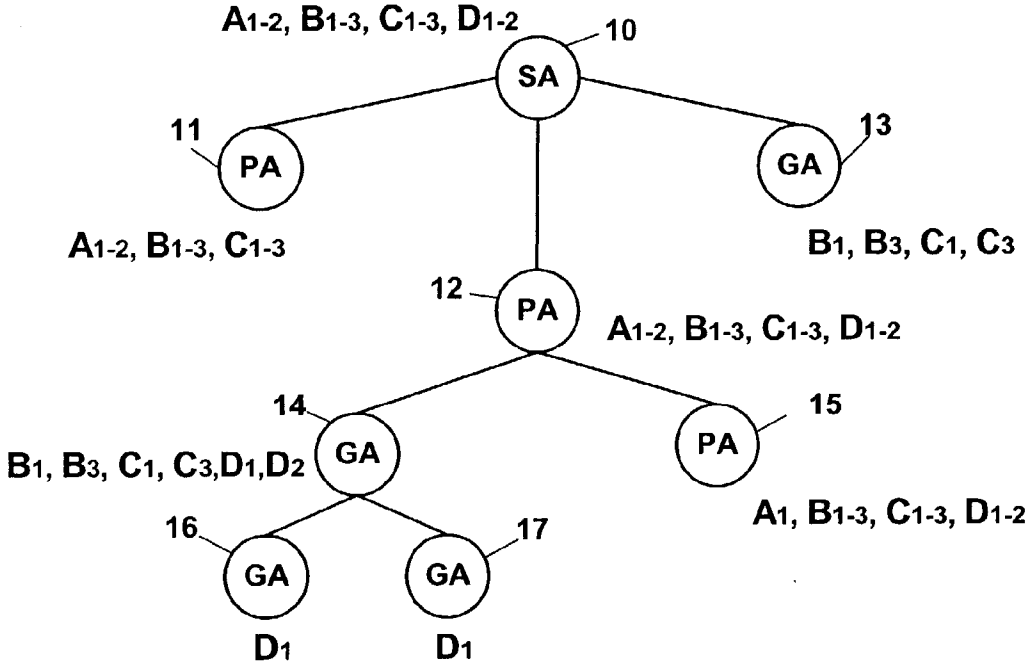

A1-2, B1-3, C1-3, D1-2
10
SA
11
PA
A1-2, B1-3, C1-3
13
GA
B1, B3, C1, C3
12
PA
A1-2, B1-3, C1-3, D1-2
14
GA
B1, B3, C1, C3,D1,D2
15
PA
A1, B1-3, C1-3, D1-2
16
GA
D1
17
GA
D1

FIG. 3

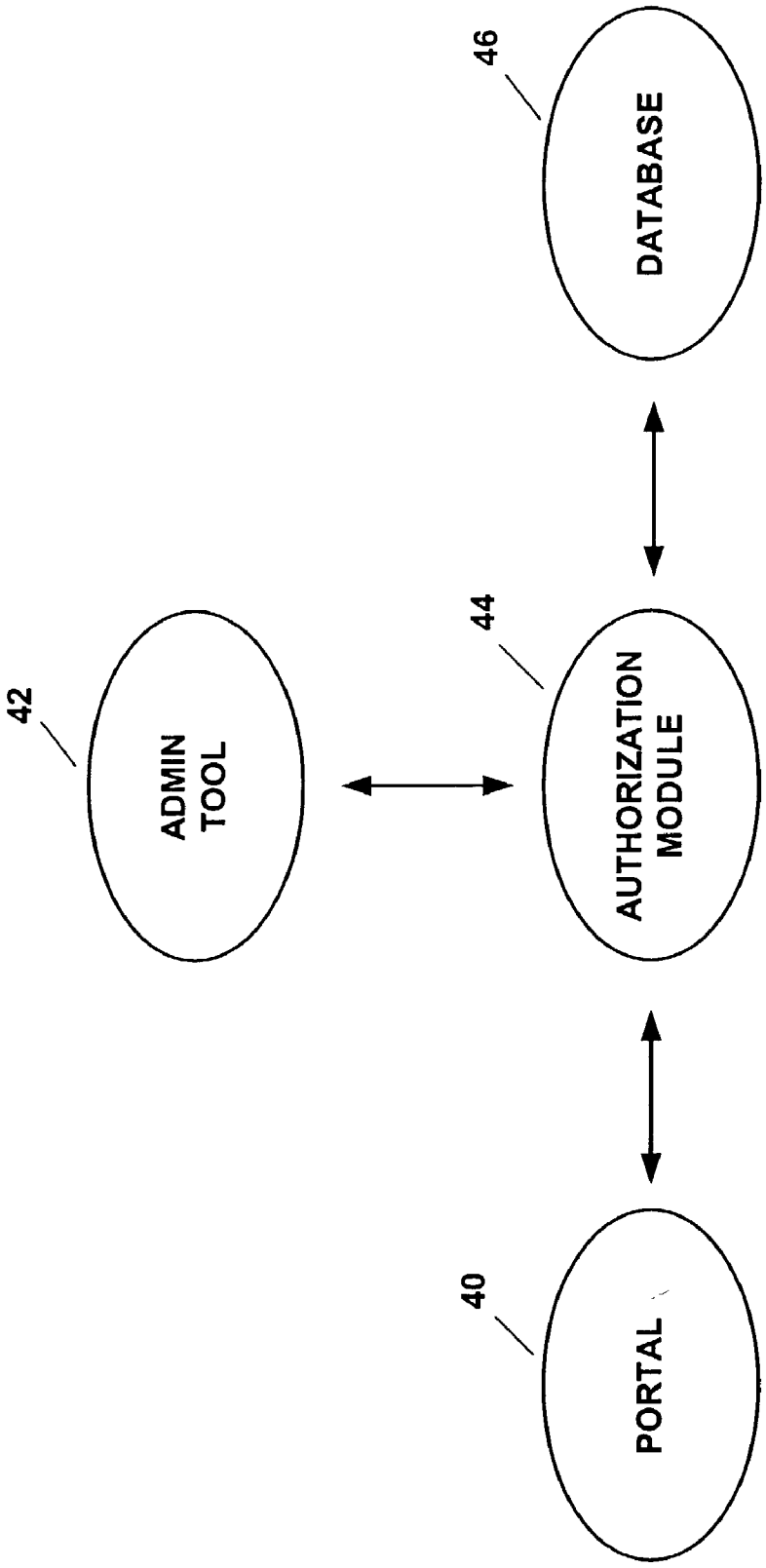

46
DATABASE
44
AUTHORIZATION MODULE
42
ADMIN TOOL
40
PORTAL

FIG. 4

SYSTEM AND METHOD FOR DELEGATED ADMINISTRATION

CROSS REFERENCES

[0002] This application is related to the following co-pending application which is hereby incorporated by reference in its entirety: SYSTEM AND METHOD FOR RULE-BASED ENTITLEMENTS, U.S. Application Serial No. _____, Inventors: Phil Griffin, et al., filed on _____.

COPYRIGHT NOTICE

FIELD OF THE DISCLOSURE

[0004] The present invention disclosure relates to the field of authorization in computer networks and, in particular, delegation of administrative privileges in an enterprise application.

BACKGROUND

[0005] Administration of an enterprise application is typically carried out by a system administrator who can perform tasks that are otherwise off-limits to non-privileged users. Such tasks can include administering user accounts, altering the layout and content of pages on a website, installing applications, running diagnostics, adding or removing components to a network, or reconfiguring a network. However, as enterprise applications grow large and complex, so do the number of administrative tasks. One way to reduce the number of tasks that a system administrator is responsible for is to distribute the tasks among a number of administrators. This approach can be problematic, however, since administrators may unwittingly perform conflicting operations. Another problem with this approach is that it increases the likelihood that the security of the enterprise application will be breached since system level privileges are entrusted to more than one individual. What is needed is a means to conveniently delegate system administration privileges while at the same time limiting the scope of such privileges.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] **FIG. 1** illustrates delegation of capabilities in accordance to one embodiment of the invention.

[0007] **FIG. 2** illustrates an administrative hierarchy in accordance to one embodiment of the invention.

[0008] **FIG. 3** illustrates delegation of administrative tasks in accordance to one embodiment of the invention.

[0009] **FIG. 4** illustrates a system in accordance to one embodiment of the invention.

DETAILED DESCRIPTION

[0010] The invention is illustrated by way of example and not by way of limitation in the figures of the accompanying drawings in which like references indicate similar elements. It should be noted that references to "an" or "one" embodiment in this disclosure are not necessarily to the same embodiment, and such references mean at least one.

[0011] In one embodiment, delegated system administration involves the conveying of a capability (e.g., the ability to perform a system administration task) from one user to another, from a process to a user, from a user to a process, or from a process to a process. A process can include, for example, a thread, a distributed object, a lightweight process, or a program of any kind that is able to execute on one or more computers. In another embodiment, a process and a user are synonymous. By way of a non-limiting illustration, the conveyed capability can include any task, operation or privilege that is able to be performed on any resource available on a computer network. For example, if a resource is a computer database, capabilities can comprise creating, reading, updating or deleting data contained therein. If the resource is an administrative task, for example, capabilities can include creating a new user account, associating an existing user account with a user group, or delegating the ability to perform a system administration task to a user.

[0012] **FIG. 1** illustrates delegation of capabilities in accordance to one embodiment of the invention. User **1** has capabilities A, B and C. User **1** has delegated these capabilities to user **2**. In doing so, user **1** also conveyed to user **2** the ability to further delegate these capabilities to others. User **1** conveyed capabilities B and C to user **3**, but with the condition that user **3** cannot further delegate C. This is indicated in **FIG. 1** by an underscore beneath the letter "C". User **2** has delegated A, B and C to user **4**, and capabilities A and B to user **5** with the condition that user **5** cannot further delegate capability B. User **3** has delegated capability B to user **6**. User **3** cannot delegate capability C. Thus, different levels of users can be created with varying degrees of system access. In one embodiment, each level of delegation can have the same capabilities. In another embodiment, each subsequent level of delegation can have the same or fewer capabilities.

[0013] A portal is a feature-rich web site. It provides a point of access to enterprise data and applications, presenting a unified and potentially personalized view of that information to employees, customers and business partners. Portals allow multiple web applications within a single web interface. In addition to regular web content that appears in a portal (e.g., text or graphics), portals provide the ability to display portlets—self-contained applications or content—all in a single web interface (e.g., a web browser). Portals also support multiple pages through navigation mechanisms (e.g., tab-based navigation) with each page containing its own content and portlets. One such system is the WebLogic® Portal, available from BEA Systems, Inc. of San Jose, Calif.

[0014] In one embodiment, a portal user can be an administrator. As such, the user can create new portals, modify the privileges of visitors and other administrators, and modify many of the attributes displayed in the portal. In another embodiment, a portal user can belong to one or more groups. Groups provide a means for organizing users with common characteristics into a single category. For example, it might be desirable to differentiate the web services offered to bank customers with large assets versus small assets in order to serve these groups better. An association between a portal

and a user group is a Group portal. Group portals allow for the definition of different views of a portal for different user groups, making it seem as if users in each group are looking at completely different web sites. Multiple group portals can be created within a single portal. In one embodiment, group portals can be managed by delegated administration.

[0015] In addition to groups, in one embodiment of the invention, users can also be organized into a hierarchy. In one embodiment, a hierarchy can include one or more users designated as system administrators (SA's), zero or more users designated as portal administrators (PA's), and zero or more users designated as group administrators (GA's). Those skilled in the art will recognize that many such hierarchies are possible. In one embodiment, an SA is able to perform all system administration tasks, whereas a PA can perform administration tasks only for a single portal, and a GA can perform administrative tasks only for a single group portal. In another embodiment, users are not organized into a hierarchy.

[0016] In one embodiment, initially there is a single user designated as an SA. The remaining users optionally belong to an "admin eligible" group. Membership in a group can be dynamically determined by evaluating rules. Users belonging to the admin eligible group can be promoted to SA, PA or GA. In another embodiment, group membership is not a prerequisite to promotion. In one embodiment, an SA can promote users in the admin eligible group to SA, PA or GA. Once promoted to SA, a user can likewise promote others to SA, PA or GA. In another embodiment, a PA can promote other users to PA or GA, and a GA can promote other users to GA. It will be apparent to those skilled in the art that user promotion can be accomplished in a number of ways, including automatically via evaluation of rules or manually via administrative tools.

[0017] **FIG. 2** illustrates an administrative hierarchy in accordance to one embodiment of the invention. SA **10** has promoted users **11** and **12** to PA and user **13** to GA. User **12** has in turn promoted user **14** to GA and user **15** to PA. User **14** in turn has promoted users **16** and **17** to GA. In one embodiment, a user cannot promote another to a role higher than itself. For example, user **14** could not promote user **16** to PA or SA. In another embodiment, users **11-17** belonged to the admin eligible group before promotion.

[0018] In one embodiment, there are four administrative tasks that an administrator (e.g., SA, PA or GA) can potentially control: user management, portal page management, portlet management and visual appearance. In one embodiment, if an administrator has the capability of managing users, the administrator can create users and optionally store information about them. In addition, an administrator can also create groups and add users to them.

[0019] In one embodiment, if an administrator has the capability of managing portal pages, the administrator can control behavioral aspects that a visitor experiences when accessing a portal, such as whether a portlet is viewed as a maximized presentation or a minimized presentation within the page of origin. If an administrator has the capability to alter the visual appearance, the administrator can modify a portal's look and feel, define and arrange the pages and portlets displayed in a portal, define the different views of the portal that different visitors see, and control access to pages and portlets within a group portal. By way of a non-limiting illustration, general portal visual characteristics can include header and footer graphics, content, icon graphics, color schemes, cascading style sheets and hypertext markup language (HTML) layouts. In another embodiment, an administrator can determine the appearance of a portal by selecting from the available skins. A skin is a collection of HTML code and graphics that affect the appearance of a portal, for example, the colors and fonts used.

[0020] In one embodiment, if an administrator has the capability of managing portlets, the administrator can define and modify the resources that are available for a portlet. The administrator can also set portlet defaults, such as whether the portlet will be available to users, whether the portlet can be minimized, whether the portlet can be maximized, etc.

[0021] Table 1 summarizes administrative tasks and their associated capabilities in one embodiment (parenthetical capability codes are provided for use in **FIG. 3**):

TABLE 1

Administrative Task Capabilities	
Task	Capabilities
User Management	Manage (A_1), Delegate (A_2)
Page Management	Manage (B_1), Delegate (B_2), Set Entitlements (B_3)
Portlet Management	Manage (C_1), Delegate (C_2), Set Entitlements (C_3)
Visual Appearance Management	Manage (D_1), Delegate (D_2)

[0022] In one embodiment, if an administrator possesses the "manage" capability, the administrator is permitted to manage the given task. If an administrator possesses the "delegate" capability, the administrator can delegate the capability to another. Finally, if an administrator has the capability "set entitlements", the administrator can define roles for dynamically associating users with resources. In one embodiment, roles allow for the definition of different views of a portal for different users. By creating groupings of characteristics, such as gender, browser type, or date, any web site visitors who match those characteristics dynamically become members of the role. Such dynamic roles are used to target visitors with campaigns and personalized content, and to control the pages and portlets web site visitors can view.

[0023] **FIG. 3** illustrates delegation of administrative tasks (see Table **1**) in accordance to one embodiment of the invention. SA **10** possesses all administrative capabilities and can delegate all of them. SA **10** has delegated a subset of these capabilities to PA **11** and GA **13**. PA **11** was granted all user, page and portlet management capabilities, but was not granted any capabilities related to visual appearance management. GA **13** was granted page and portlet management capabilities, but does not have the capability to delegate these (i.e., B_2 and C_2). GA **13** was not granted any capabilities related to user or visual appearance management. PA **12** was granted the full set of capabilities from SA **10** and in turn granted a subset of these to GA **14** and PA **15**. GA **14** was only granted delegation capability for managing visual appearance, and thus was able to delegate this capability to GA **16** and GA **17**. GA **16** and GA **17** cannot delegate D_1 since they lack D_2. PA **15** was delegated all capabilities except the ability to delegate user management (A_2). Therefore, PA **15** can delegate B_{1-3}, C_{1-3} and D_{1-3}, but not A_1.

[0024] In one embodiment, delegated administration can be implemented using entitlements. An entitlement is a mechanism for dynamically associating capabilities with a user. In one embodiment, an entitlement includes a resource, a capability, a permission, and a role rule. For example, if evaluation of a role rule places a user in the role of SA, PA or GA, that user then possesses the capability associated with the resource, assuming that the permission allows it. A permission in one embodiment can be grant, deny or abstain. A resource can include any resource available on a computer network and, in another embodiment, a resource can include logical resources.

[0025] In one embodiment, resource names can be arranged in a taxonomy. A taxonomy provides a means of categorizing and uniquely identifying a resource and is hierarchical in nature. For example, a resource name could be "myPortal.bankerGroup.pageMgmt.smith". In this example, "myPortal" is the top level taxonomy name and serves to indicate that the resource is a portal named "myPortal". The next part of the resource name, "bankerGroup", identifies a user group associated with the portal "myPortal" consisting of bankers. The third part of the resource name indicates an administrative task (i.e., page management) for the group portal "bankerGroup". Finally, the last part of the resource name identifies a particular user, "smith". Thus, the resource name in this example identifies a user "smith" that has been delegated at least one capability associated with page administration, wherein the page administration is for the group portal "bankerGroup" within portal "myPortal".

[0026] In one embodiment, a role rule is defined in terms of one or more logical expressions. A role rule of "everyone" is provided as a default and evaluates to "true" for any user. In another embodiment, a role rule can be based on evaluation of predicates. A predicate is a rule that evaluates to true or false. By way of a non-limiting example, predicates may include other predicates, logical operators (e.g., AND, NOT and OR), mathematical operations, method calls, calls to external systems, function calls, etc. In another embodiment, rules can be specified in plain English. For example:

[0027] When all of these conditions apply, the user is a groupAdmin:

[0028] Administrative Skill Level at least 5

[0029] Trustworthiness is 'High'

[0030] Time of day is between 12:00 am and 6:00 am.

[0031] In the example above, the role that is being determined is "groupAdmin". The predicate "Administrative Skill Level is at least 5" evaluates to true when a user's predefined administration level is set to five or higher. The "Trustworthiness is High" predicate evaluates to true if, for example, a predefined trustworthiness level is set to high. The "Time of day" predicate evaluates to "true" if the time of day is between 12:00 am and 6:00 am. It will be apparent to those skilled in the art that any type of predicate can be included in a role rule. To summarize, this role rule allows a user to become a group administrator if their skill level is at least five, they are trustworthy and it is the middle of the night.

TABLE 2

Administrative Task Entitlements

Resource Name	Capability	Role	Perm
myPortal.bankerGroup.userMgmt	manage (A_1)	groupAdmin	deny
myPortal.bankerGroup.userMgmt	delegate (A_2)	groupAdmin	deny
myPortal.bankerGroup.pageMgmt	manage (B_1)	groupAdmin	grant
myPortal.bankerGroup.pageMgmt	delegate (B_2)	groupAdmin	deny
myPortal.bankerGroup.pageMgmt	entitlements (B_3)	groupAdmin	grant
myPortal.bankerGroup.portletMgmt	manage (C_1)	groupAdmin	grant
myPortal.bankerGroup.portletMgmt	delegate (C_2)	groupAdmin	deny
myPortal.bankerGroup.portletMgmt	entitlements (C_3)	groupAdmin	grant
myPortal.bankerGroup.visualMgmt	manage (D_1)	groupAdmin	deny
myPortal.bankerGroup.visualMgmt	delegate (D_2)	groupAdmin	deny

[0032] In one embodiment, by way of example, exemplary entitlements for GA **13** in **FIG. 3** are listed in Table 2. The resource name indicates the portal, group portal, and administrative task for that group portal. The capability is a particular capability associated with the administrative task, as in Table 1. The role rule being evaluated is groupAdmin, as above. Finally, the last column in the table is the permission associated with the capability. Notice that GA **13** was not granted any capabilities related to user or visual appearance management, or delegation of portal and portlet management. These entitlements have a permission of "deny". Thus, a user who dynamically satisfies the role rule groupAdmin will be entitled to the granted capabilities associated with this role.

[0033] In another embodiment, by way of illustration, a user is associated with an administrative role by incorporating the user's name in the resource name. Exemplary entitlements for GA **13** in **FIG. 3** in this embodiment are listed in Table 3.

TABLE 3

Administrative Task Entitlements

Resource Name	Capability	Role	Perm
MyPortal.bankerGroup.userMgmt.smith	manage (A_1)	everyone	deny
MyPortal.bankerGroup.userMgmt.smith	delegate (A_2)	everyone	deny
MyPortal.bankerGroup.pageMgmt.smith	manage (B_1)	everyone	grant
MyPortal.bankerGroup.pageMgmt.smith	delegate (B_2)	everyone	deny
MyPortal.bankerGroup.pageMgmt.smith	entitlements (B_3)	everyone	grant
MyPortal.bankerGroup.portletMgmt.smith	manage (C_1)	everyone	grant
MyPortal.bankerGroup.portletMgmt.smith	delegate (C_2)	everyone	deny
MyPortal.bankerGroup.portletMgmt.smith	entitlements (C_3)	everyone	grant

TABLE 3-continued

Administrative Task Entitlements			
Resource Name	Capability	Role	Perm
MyPortal.bankerGroup. visualMgmt.smith	manage (D_1)	everyone	deny
MyPortal.bankerGroup. visualMgmt.smith	delegate (D_2)	everyone	deny

[0034] Since the role rule is "everyone", every user will satisfy the role. Therefore, discrimination among users is based on the resource which includes a user name. When evaluating entitlements in Table 3, the resource name is incorporated with the name of the user under consideration. In this example, if the user is "smith", the user will be entitled to the same capabilities as the groupAdmin in Table 2.

[0035] In another embodiment, a user is associated with an administrative role (e.g., SA, PA or GA) through a mapping between users and administrators. Those skilled in the art will recognize that such a mapping can be implemented in a number of ways, including a database table, a cache, a function, or any combination thereof. In yet another embodiment, a user can be identified as an administrator based on group membership. For example, an SA belongs to the SA group, etc.

[0036] **FIG. 4** illustrates a system in accordance to one embodiment of the invention. In one embodiment, by way of example, a portal user (not shown) accesses portal **40** through a web browser, such as Microsoft® Internet Explorer available from Microsoft Corp. of Redmond, Wash. The user logs into the portal by typing a login name and password. This information is sent to authorization and authentication module **44** which responds with a set of groups (not shown) for the user. Portal **40** can use the group information to customize the look and feel of the portal page(s) presented to the user. If a user is an administrator, the user can alternately log into admin tool **42** (e.g., via a web browser). Admin tool **42** allows an administrator to perform delegation, promotion, define groups, role rules and entitlements. Of course, a given administrator is limited in what they can do based on their capabilities. When an administrator logs into admin tool **42**, this information is sent to the authorization module which returns a set of capabilities based on the evaluation of one or more role rules. Authorization module **44** can utilize database **46** to persist information related to users, groups, entitlements, capabilities, resources, and role rules. In one embodiment, database **46** can be a relational database, an object-oriented database, a flat file, a cache or any other data structure that allows storage and access information. In determining capabilities, authorization module **44** can evaluate one or more role rules to determine which entitlements are appropriate for a user. In another embodiment, all components in **FIG. 4** may be part of the same software module. In another embodiment, the components may be arbitrarily grouped into different software modules. All components shown in **FIG. 4** may reside on the same system or, in another embodiment, may be distributed in a computer network.

[0037] The foregoing description of the preferred embodiments of the present invention has been provided for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise forms disclosed. Many modifications and variations will be apparent to the practitioner skilled in the art. Embodiments were chosen and described in order to best describe the principles of the invention and its practical application, thereby enabling others skilled in the art to understand the invention, the various embodiments and with various modifications that are suited to the particular use contemplated. It is intended that the scope of the invention be defined by the following claims and their equivalents.

What is claimed is:

1. A method for delegating portal administrative authority, comprising:

determining at least one capability for a first user based on evaluation of at least one role rule; and

delegating the at least one capability to a second user; and

wherein the delegation establishes whether or not the second user can delegate the capability.

2. The method of claim 1 wherein:

the delegated at least one capability is a subset of the at least one capability for the first user.

3. The method of claim 1 wherein:

the at least one capability is one of: user management, page management, portlet management, portal entitlement management, portlet entitlement management, and visual appearance management.

4. The method of claim 1 wherein:

the first user and the second user have a hierarchical relationship and the second user is hierarchically equal or subordinate to the first user.

5. The method of claim 1 wherein:

the second user is promoted by the first user.

6. The method of claim 1 wherein:

the at least one role rule defaults to everyone.

7. The method of claim 1 wherein:

the at least one role rule is associated with an entitlement.

8. The method of claim 7 wherein:

the entitlement includes a resource name and a permission.

9. The method of claim 8 wherein:

the resource name is part of a taxonomy.

10. The method of claim 8 wherein:

the resource name identifies the first user.

11. The method of claim 1 wherein:

the at least one role rule includes at least one predicate.

12. The method of claim 1 wherein:

the at least one role rule is specified in plain language.

13. The method of claim 1 wherein:

the at least one role rule associates the first user with a role.

14. The method of claim 13 wherein:

the role is one of System Administrator, Portal Administrator, and Group Administrator.

15. The method of claim 1 wherein:

the second user belongs to a group whose members can be promoted.

16. A method for delegating portal administrative authority, comprising:

determining at least one capability for a first user based on evaluation of at least one role rule; and

delegating the at least one capability to a second user; and

wherein the delegated at least one capability is a subset of the at least one capability of the first user.

17. The method of claim 16 wherein:

the first user controls whether the second user can delegate the at least one capability to a third user.

18. The method of claim 16 wherein:

the at least one capability is one of: user management, page management, portlet management, portal entitlement management, portlet entitlement management, and visual appearance management.

19. The method of claim 16 wherein:

the first user and the second user have a hierarchical relationship and the second user is hierarchically equal or subordinate to the first user.

20. The method of claim 16 wherein:

the second user is promoted by the first user.

21. The method of claim 16 wherein:

the at least one role rule defaults to everyone.

22. The method of claim 16 wherein:

the at least one role rule is associated with an entitlement.

23. The method of claim 22 wherein:

the entitlement includes a resource name and a permission.

24. The method of claim 23 wherein:

the resource name is part of a taxonomy.

25. The method of claim 23 wherein:

the resource name identifies the first user.

26. The method of claim 16 wherein:

the at least one role rule includes at least one predicate.

27. The method of claim 16 wherein:

the at least one role rule is specified in plain language.

28. The method of claim 16 wherein:

the at least one role rule associates the first user with a role.

29. The method of claim 28 wherein:

the role is one of System Administrator, Portal Administrator, and Group Administrator.

30. The method of claim 16 wherein:

the second user belongs to a group whose members can be promoted.

31. A method for delegating portal administrative authority, comprising:

determining for a first user at least one task having at least one capability; and

delegating the at least one capability from the first user to at least one other user; and

wherein the delegated at least one capability is a subset of the at least one capability of the first user.

32. The method of claim 31 wherein:

determining for a first user at least one task having at least one capability includes evaluting at least one role rule.

33. The method of claim 31 wherein:

the at least one capability is one of: user management, page management, portlet management, portal entitlement management, portlet entitlement management, and visual appearance management.

34. The method of claim 31 wherein:

the first user and the at least one other user have a hierarchical relationship and the at least one other user is hierarchically equal or subordinate to the first user.

35. The method of claim 31 wherein:

the at least one other user is promoted by the first user.

36. The method of claim 32 wherein:

the at least one role rule defaults to everyone.

37. The method of claim 32 wherein:

the at least one role rule is associated with an entitlement.

38. The method of claim 37 wherein:

the entitlement includes a resource name and a permission.

39. The method of claim 38 wherein:

the resource name is part of a taxonomy.

40. The method of claim 38 wherein:

the resource name identifies the first user.

41. The method of claim 32 wherein:

the at least one role rule includes at least one predicate.

42. The method of claim 32 wherein:

the at least one role rule is specified in plain language.

43. The method of claim 32 wherein:

the at least one role rule associates the first user with a role.

44. The method of claim 43 wherein:

the role is one of System Administrator, Portal Administrator, and Group Administrator.

45. The method of claim 31 wherein:

the at least one other user belongs to a group whose members can be promoted.

46. A method for delegating authority, comprising:

determining for a first user at least one task having at least one capability based on at least one entitlement; and

delegating the at least one capability from the first user to at least one other user; and

wherein the delegated at least one capability is a subset of the first user's capabilities.

47. The method of claim 46 wherein:

determining for a first user at least one task having at least one capability includes evaluating at least one role rule.

48. The method of claim 46 wherein:

the delegated at least one capability is a subset of the at least one capability for the first user.

49. The method of claim 46 wherein:

the at least one capability is one of: user management, page management, portlet management, portal entitlement management, portlet entitlement management, and visual appearance management.

50. The method of claim 46 wherein:

the first user and the at least one other user have a hierarchical relationship and the at least one other user is hierarchically equal or subordinate to the first user.

51. The method of claim 46 wherein:

the at least one other user is promoted by the first user.

52. The method of claim 47 wherein:

the at least one role rule defaults to everyone.

53. The method of claim 46 wherein:

the entitlement includes a resource name and a permission.

54. The method of claim 53 wherein:

the resource name is part of a taxonomy.

55. The method of claim 53 wherein:

the resource name identifies the first user.

56. The method of claim 47 wherein:

the at least one role rule includes at least one predicate.

57. The method of claim 47 wherein:

the at least one role rule is specified in plain language.

58. The method of claim 47 wherein:

the at least one role rule associates the first user with a role.

59. The method of claim 58 wherein:

the role is one of System Administrator, Portal Administrator, and Group Administrator.

60. The method of claim 46 wherein:

the at least one other user belongs to a group whose members can be promoted.

61. A system for delegating authority, comprising:

an authorization module to determine at least one capability associated with a first user based on evaluation of at least one role rule; and

an administration tool coupled to the authorization module, the administration tool to delegate the at least one capability from the first user to a second user.

62. The system of claim 61 wherein:

the first user controls whether the second user can delegate the at least one capability to a third user.

63. The system of claim 61 wherein:

the delegated at least one capability is a subset of the at least one capability for the first user.

64. The system of claim 61 wherein:

the at least one capability is one of: user management, page management, portlet management, portal entitlement management, portlet entitlement management, and visual appearance management.

65. The system of claim 61 wherein:

the first user and the second user have a hierarchical relationship and the second user is hierarchically equal or subordinate to the first user.

66. The system of claim 61 wherein:

the second user is promoted by the first user.

67. The system of claim 61 wherein:

the at least one role rule defaults to everyone.

68. The system of claim 61 wherein:

the at least one role rule is associated with an entitlement.

69. The system of claim 68 wherein:

the entitlement includes a resource name and a permission.

70. The system of claim 69 wherein:

the resource name is part of a taxonomy.

71. The system of claim 68 wherein:

the resource name identifies the first user.

72. The system of claim 61 wherein:

the at least one role rule includes at least one predicate.

73. The system of claim 61 wherein:

the at least one role rule is specified in plain language.

74. The system of claim 61 wherein:

the at least one role rule associates the first user with a role.

75. The system of claim 74 wherein:

the role is one of System Administrator, Portal Administrator, and Group Administrator.

76. The system of claim 61 wherein:

the second user belongs to a group whose members can be promoted.

77. A machine readable medium having instructions stored thereon that when executed by a processor cause a system to:

determine at least one capability for a first user based on evaluation of at least one role rule; and

delegate the at least one capability to a second user.

78. The machine readable medium of claim 77 wherein:

the first user controls whether the second user can delegate the at least one capability to a third user.

79. The machine readable medium of claim 77 wherein:

the delegated at least one capability is a subset of the at least one capability for the first user.

80. The machine readable medium of claim 77 wherein:

the at least one capability is one of: user management, page management, portlet management, portal entitlement management, portlet entitlement management, and visual appearance management.

81. The machine readable medium of claim 77 wherein:

the first user and the second user have a hierarchical relationship and the second user is hierarchically equal or subordinate to the first user.

82. The machine readable medium of claim 77 wherein:

the second user is promoted by the first user.

83. The machine readable medium of claim 77 wherein:

the at least one role rule defaults to everyone.

84. The machine readable medium of claim 77 wherein:

the at least one role rule is associated with an entitlement.

85. The machine readable medium of claim 84 wherein:

the entitlement includes a resource name and a permission.

86. The machine readable medium of claim 85 wherein:

the resource name is part of a taxonomy.

87. The machine readable medium of claim 85 wherein:

the resource name identifies the first user.

88. The machine readable medium of claim 77 wherein:

the at least one role rule includes at least one predicate.

89. The machine readable medium of claim 77 wherein:

the at least one role rule is specified in plain language.

90. The machine readable medium of claim 77 wherein:

the at least one role rule associates the first user with a role.

91. The machine readable medium of claim 90 wherein:

the role is one of System Administrator, Portal Administrator, and Group Administrator.

92. The machine readable medium of claim 77 wherein:

the second user belongs to a group whose members can be promoted.

93. The method of claims **77** wherein:

the step of delegating can limit the scope of the capability delegated.

94. The method of claims **77** wherein:

the delegating step can limit the capability delegated to one or more of a manage capability, a delegate capability and a set entitlements capability.

95. A system for delegating authority, comprising:

an authorization module to determine at least one capability associated with a first user based on evaluation of at least one role rule; and

an administration tool coupled to the authorization module, the administration tool to delegate the at least one capability from the first user to a second user; and

wherein the first user controls whether the second user can delegate the at least one capability to a third user; and

wherein the at least one role rule is associated with an entitlement.

96. The system of claim 95 wherein:

the delegated at least one capability is a subset of the at least one capability for the first user.

97. The system of claim 95 wherein:

the at least one capability is one of: user management, page management, portlet management, portal entitlement management, portlet entitlement management, and visual appearance management.

98. The system of claim 95 wherein:

the first user and the second user have a hierarchical relationship and the second user is hierarchically equal or subordinate to the first user.

99. The system of claim 95 wherein:

the second user is promoted by the first user.

100. The system of claim 95 wherein:

the at least one role rule defaults to everyone.

101. The system of claim 95 wherein:

the entitlement includes a resource name and a permission.

102. The system of claim 101 wherein:

the resource name is part of a taxonomy.

103. The system of claim 101 wherein:

the resource name identifies the first user.

104. The system of claim 95 wherein:

the at least one role rule includes at least one predicate.

105. The system of claim 95 wherein:

the at least one role rule is specified in plain language.

106. The system of claim 95 wherein:

the at least one role rule associates the first user with a role.

107. The system of claim 106 wherein:

the role is one of System Administrator, Portal Administrator, and Group Administrator.

108. The system of claim 95 wherein:

the second user belongs to a group whose members can be promoted.

109. A machine readable medium having instructions stored thereon that when executed by a processor cause a system to:

determine for a first user at least one task having at least one capability based on at least one entitlement; and

delegate the at least one capability from the first user to at least one other user; and

wherein the delegated at least one capability is a subset of the first user's capabilities.

110. The machine readable medium of claim 109 wherein:

the first user controls whether the at least one other user can delegate the at least one capability to a third user.

111. The machine readable medium of claim 109 wherein:

the at least one capability is one of: user management, page management, portlet management, portal entitlement management, portlet entitlement management, and visual appearance management.

112. The machine readable medium of claim 109 wherein:

the first user and the at least one other user have a hierarchical relationship and the at least one other user is hierarchically equal or subordinate to the first user.

113. The machine readable medium of claim 109 wherein:

the at least one other user is promoted by the first user.

114. The machine readable medium of claim 109 wherein:

the at least one entitlement includes a resource name and a permission.

115. The machine readable medium of claim 114 wherein:

the resource name is part of a taxonomy.

116. The machine readable medium of claim 114 wherein:

the resource name identifies the first user.

117. The machine readable medium of claim 109 wherein:

the at least one entitlement includes at least one role rule.

118. The machine readable medium of claim 117 wherein:

the at least one role rule includes at least one predicate.

119. The machine readable medium of claim 117 wherein:

the at least one role rule is specified in plain language.

120. The machine readable medium of claim 117 wherein:

the at least one role rule associates the first user with a role.

121. The machine readable medium of claim 120 wherein:

the role is one of System Administrator, Portal Administrator, and Group Administrator.

122. The machine readable medium of claim 109 wherein:

the at least one other user belongs to a group whose members can be promoted.

123. The method of claims **109** wherein:

the step of delegating can limit the scope of the capability delegated.

124. The method of claims **109** wherein:

the delegating step can limit the capability delegated to one or more of a manage capability, a delegate capability and a set entitlements capability.

* * * * *