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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 September 2004 (02.09.2004)

PCT

(10) International Publication Number
WO 2004/074994 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/US2004/004079

(22) International Filing Date: 12 February 2004 (12.02.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/367,462 14 February 2003 (14.02.2003) US

(71) Applicant *(for all designated States except US)*: **BEA SYSTEMS, INC.** [US/US]; 2315 North First Street, San Jose, CA 95131 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **GRIFFIN, Philip, B.** [US/US]; 6620 Fairways Drive, Longmont, CO 80503 (US). **DEVGAN, Manish** [IN/US]; 1405 Snowberry Lane, Broomfield, CO 80020 (US). **TOUSSAINT, Alex** [BR/US]; 765 Eldorado Boulevard, 2226, Broomfield, CO 80021 (US). **MCCAULEY, Rod** [US/US]; 2474 Mary Beth Court, Loveland, Colorado 80537 (US).

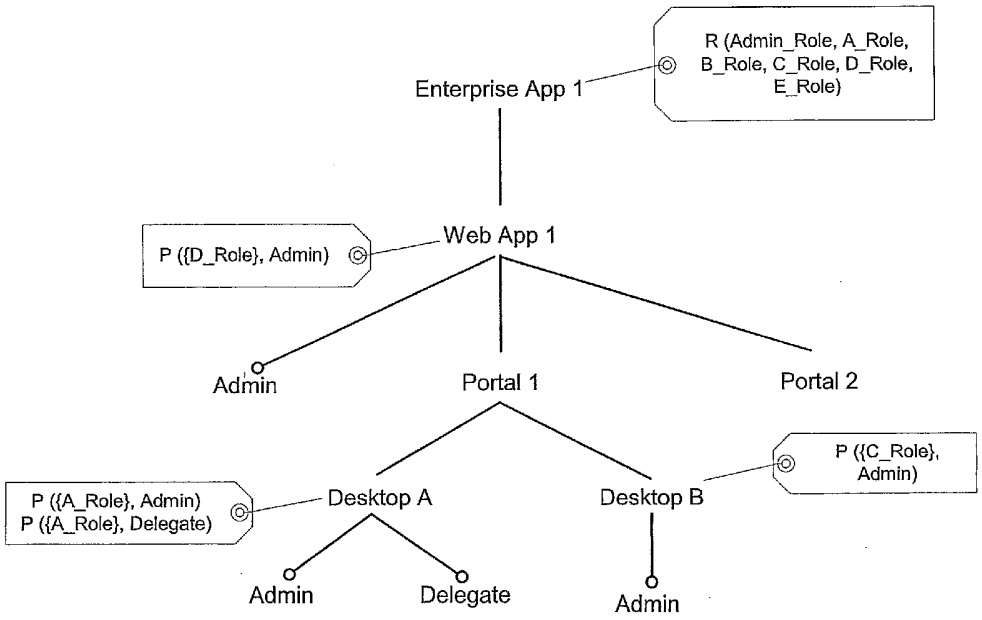
(74) Agents: **MEYER, Sheldon, R.** et al.; Fliesler Meyer LLP, Four Embarcadero Center, Fourth Floor, San Francisco, CA 94111-4156 (US).

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

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

[Continued on next page]

(54) Title: METHOD FOR ROLE AND RESOURCE POLICY MANAGEMENT



(57) Abstract: A method for adaptively managing entitlements, comprising the steps of providing for the association of a role with a first resource; and providing for the association of a policy with a second resource, wherein the policy is based at least partially on the role; and providing for hierarchically relating the role and the policy; and wherein the role is hierarchically equal or superior to the policy.

WO 2004/074994 A2

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, 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)*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*

Published:

— *without international search report and to be republished upon receipt of that 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.

METHOD FOR ROLE AND RESOURCE POLICY MANAGEMENT

COPYRIGHT NOTICE

CROSS REFERENCES

This application is related to the following co-pending applications which are hereby incorporated by reference in their entirety: SYSTEM AND METHOD FOR HIERARCHICAL ROLE-BASED ENTITLEMENTS, U.S. Application Serial No. 10/367,177, Inventors: Philip B. Griffin, et al., filed on February 14, 2003; METHOD FOR DELEGATED ADMINISTRATION, U.S. Application Serial No. 10/367,190, Inventors: Philip B. Griffin, et al., filed on February 14, 2003; and METHOD FOR ROLE AND RESOURCE POLICY MANAGEMENT OPTIMIZATION, U.S. Application Serial No. 10/366,778, Inventor: Philip B. Griffin, filed on February 14, 2003.

FIELD OF THE DISCLOSURE

The present invention disclosure relates to authorization and control of resources in an enterprise application.

BACKGROUND

Enterprise applications can increase the availability of goods and services to customers inside and outside of an organization. One issue that accompanies deployment of an enterprise application is authorization or access control. Both customers and system administrators need to be privileged to

perform certain actions (e.g., modifying a customer account) or to gain access to certain content. Typical authorization systems can be complex and time consuming to implement and maintain, especially if they are tied closely to the business logic in an enterprise application.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is an illustration of a exemplary resource hierarchy in accordance to one embodiment of the invention.

Figure 2 is the exemplary hierarchy of **Figure 1** further illustrating roles and security policies.

Figure 3 is a diagram of an authorization system in accordance to one embodiment of the invention.

Figure 4 is an illustration of a delegation role hierarchy in accordance to one embodiment of the invention.

Figure 5 is an illustration of exemplary delegation security policies in one embodiment of the invention.

DETAILED DESCRIPTION

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.

In one embodiment, an enterprise application includes one or more resources that facilitate the performance of business, scientific or other functions and tasks. In another embodiment, an enterprise application can be a Java™ 2 Enterprise Edition (J2EE) deployment unit that bundles together Web Applications, Enterprise Java™ Beans and Resource Adaptors into a single deployable unit. The Java™ programming language and its run-time libraries and environment are available from Sun Microsystems, Inc., of Santa Clara,

California. Enterprise applications can include software, firmware and hardware elements. Software, firmware and hardware can be arbitrarily combined or divided into separate logical components. Furthermore, it will be apparent to those skilled in the art that such components, irregardless of how they are combined or divided, can execute on the same computer or can be arbitrarily distributed among different computers connected by one or more networks.

In one embodiment, a resource can correspond to any person, place or thing, including an object or an entity (e.g., a network, a computer, a computer user, a bank account, an electronic mail message, aspects of a computer operating system such as virtual memory, threads and file storage, etc.), a method or a process (e.g., balancing a checkbook, installing a device driver, allocating virtual memory, deleting a file, etc.), the occurrence or non-occurrence of an event (e.g., an attempt by a user to logon to a computer, a change in state, etc.) and an organization or association of resources (e.g., lists, trees, maps, hierarchies, etc.).

In one embodiment, resources can be classified into a hierarchical taxonomy (which itself can be a resource). By way of a non-limiting example, in an enterprise application, it may be necessary to refer to a particular resource such as a booklet. In order to reference the booklet, one needs to know which web page it is on, which portal the web page belongs to, which web application (or "web app") owns the web page, and which domain the web app belongs to. Each of these components is considered a resource and can be described as a resource path (e.g., a sequence of components separated by slashes):

```
domain/web_app/portal/desktop/page/booklet
```

The first resource is *domain* which lies at the "top" of the resource hierarchy. Working down the hierarchy, the next component is *web_app*. The *web_app* is a "child" or "descendent" of *domain* and *domain* is a "parent" of

web_app. The *domain* is superior to *web_app* and *web_app* is inferior to *domain*. Likewise, *portal* is a child of *web_app* and a parent of *desktop*. The *page* is a child of *desktop* with *booklet* as its child. The depth of the resource is the number of components in its path. For example, the depth of *booklet* is six (assuming that we are counting from 1) and the depth of *portal* is three. In one embodiment, the depth of a resource can be unlimited. In one embodiment, a resource can have properties or capabilities. By way of a non-limiting example, a booklet resource could have the ability to be customized by an end-user. The capability could be appended to the hierarchy as follows:

```
domain/web_app/portal/desktop/page/booklet.customize
```

Figure 1 is an illustration of an exemplary resource hierarchy in accordance to one embodiment of the invention. By way of a non-limiting example, this hierarchy can represent resources within an enterprise application. *Web App 1* and *Web App 2* are Web applications. A Web application resource is a part of an enterprise application that is accessible on the World Wide Web. *Portal 1* and *Portal 2* are portal resources and are children of *Web App 1*. *Portal 3* is a child of *Web App 2*. In one embodiment, *Web App 1* and *Web App 2* can be children of one or more enterprise applications (not shown) which can be children of one or more domains (not shown). A portal is a point of access to data and applications that provides a unified and potentially personalized view of information and resources. Typically, a portal is implemented as one or more pages on a website (*Page 1, Page 2, Page A, Page B, Page X,* and *Page Y).* Portal pages can integrate many elements, such as applications, live data feeds, static information and multimedia presentations.

Desktop A, *Desktop B* and *Desktop C* contain one or more views of a portal that have been customized for a particular user or group of users. Pages within each desktop can contain portlets (*Portlet A, Portlet B*, and *Portlet C*) and booklets (*Booklet 1* and *Booklet 2*). A portlet is a self-contained application

that renders itself on a portal page. In one embodiment, a booklet is a collection of one or more pages or booklets. Resource *Web App 1/Portal 1/Desktop A/Page 2/Booklet 1/Page A* has a capability *Cap 3*. Likewise, *Web App 1/Portal 1/Desktop A/Page 2/Booklet 1/Booklet 2* has a capability *Cap 4* and *Web App 1/Portal 1/Desktop A/Page 2/Booklet 1/Booklet 2/Page Y/Portlet A* has capabilities *Cap 1* and *Cap 2*.

Enterprise applications can control access to their resources and/or capabilities through the use of entitlements. In one embodiment, evaluation of an entitlement consists of determining a security policy by dynamically associating one or more roles with a principal. In one embodiment, a role can be based on rules that take into account information including knowledge about the principal, knowledge about a communication session, the current state of the system, and/or any other relevant information.

In one embodiment, a user represents a person who uses an enterprise application. A group can be an arbitrary collection of users. In one embodiment, members of a group share common traits such as job title, etc. A process can be a software or firmware computer program or portion thereof of any granularity (e.g., a task, thread, lightweight process, distributed object, Enterprise Java™ Bean, or any other computing operation). Users, groups and processes can be considered subjects. Subjects can be authenticated based on providing adequate proof (e.g., password, social security number, etc.) to an authentication system. Once authenticated, a subject can be considered a principal for purposes of evaluating entitlements. A principal is an identity assigned to a user, group or process as a result of authentication. A principal can also represent an anonymous user, group or process (e.g., a subject that has not been authenticated).

In one embodiment, a role definition contains one or more expressions that evaluate to true or false when evaluated for a given principal in a given context. In another embodiment, an expression can evaluate to a degree of certainty that access to a resource should be granted. Expressions may be

nested within each other and can contain functions, arithmetic or logical operators, etc. In one embodiment, expressions are combined (e.g., with Boolean operators such as "and", "or", and "not") to form a Boolean expression that evaluates to true or false. If a role evaluates to true, then the principal in question is considered to satisfy the role.

Role expressions can be dynamically evaluated against a principal attempting to access a resource in a given context. A context can contain any information relevant to making a determination of whether a principal belongs in a role. By way of a non-limiting example, a context can include any of a principal's attributes (e.g., name, age, address, etc.) and/or information about a communication session. In another embodiment, a context can include information from a hypertext transfer protocol ("HTTP") or hypertext transfer protocol (secure) (HTTPS) request. This information can pertain to character encoding, remote user, authorization scheme, content length, server port, context path, request URI, request method, scheme, servlet path, content type, remote host, request protocol, locale, server name, remote address, query string, path information, etc. It will be apparent to those skilled in the art that a context can include *any* information which is relevant to evaluating an expression.

In one embodiment, expressions can include predicates. The invention disclosed herein is not limited to the present predicates discussed. A *user* predicate evaluates to true if the principal in question is the principal supplied as an argument to the predicate. The *group* predicate evaluates to true if the principal in question is a member of the specified group.

ROLE	EXPRESSION
Anonymous	*Satisfied by all principals*
BankManager	(User = Donna)
CustomerService	(User = Michael or Peter) or (Group = BankTellers)
LoanOfficer	(Group = Associate) and (Group = TrainingLevel2) and not (User = Bob)
BankManager	(User = Donna) and ((10/14/02 <= currentDate <= 10/25/02) or (11/14/02 <= currentDate <= 11/25/02))

Software	(Segment = JavaDeveloper)
SysAdmin	((User = Donna) and ((10/14/02 <= currentDate <= 10/25/02) or (11/14/02 <= currentDate <= 11/25/02))) or (Segment = SystemAdministrator)

Table 1: Exemplary Roles

Table 1 illustrates seven exemplary roles and their accompanying expressions. In one embodiment, the role "Anonymous" is a special role that is always satisfied. In another embodiment, the role of "Anonymous" is satisfied by an unauthenticated principal. The role of "BankManager" is met by a principal that is authenticated as user "Donna". The role of "CustomerService" is fulfilled by a principal authenticated as "Michael" or "Peter", or belonging to group "BankTellers". The "LoanOfficer" role is met by a principal that is a member of both the "Associate" group and the "TrainingLevel2" group, but is not "Bob". Roles can also be dynamic. By way of a non-limiting example, a role can be date and/or time dependent. In one embodiment, a time period can be specified using the *currentDate* predicate. The role of "BankManager" can be fulfilled by "Donna", but only between October 14, 2002 – October 25, 2002 or November 14, 2002 – November 25, 2002. It will be apparent to those skilled in the art that many such date or time predicates are possible (e.g., a predicate that is based on a date and a time, or one that is based on time only, etc.).

In addition to the predicates discussed above, a *segment* predicate (hereafter referred to as a "segment") can also be included in a role definition. A segment evaluates to true if the principal in question satisfies the segment's criteria. A segment can be defined in terms of one or more expressions or conditions which can be nested and include logical operators, mathematical operations, method calls, calls to external systems, function calls, etc. In another embodiment, a segment can be specified in plain language. By way of a non-limiting example:

```
When all of these conditions apply, the principal is a
JavaDeveloper:
      Developer is equal to True
      Skill level is equal to 'High'
      Preferred language is equal to 'Java'
```

In this example, the segment being described is "ExperiencedJavaDeveloper". The condition "Developer is equal to True" will evaluate to true when information contained in or referenced through a context indicates that the principal in question is a user in the software development department of an organization. Likewise, the other conditions ("Skill level is equal to 'High'", "Preferred language is equal to 'Java'") could similarly be evaluated using information from or referenced through a context. In another embodiment, a condition can pertain to information about a communication session. It will be apparent to those skilled in the art that a condition can be based on *any* information, whether the information is connected with a particular principal or not. If the segment as a whole evaluates to true, the principal is said to have satisfied the segment. In **Table 1**, by way of a non-limiting example, the role of "Software" is met by a principal that satisfies the "JavaDeveloper" segment.

By way of a further non-limiting example:

```
When all of these conditions apply, the principal is a
SystemAdministrator:
      TimeofDay is between 12:00am and 7:00am
      SystemLoad is 'Low'
      AdminSkillLevel is at least 5
```

In this example, two conditions ("TimeofDay is between 12:00am and 7:00am" and "SystemLoad is 'Low'") are based on information unrelated to a particular principal. The segment evaluates to true for the principal in question if it is the middle of the night, the system is not busy, and the principal has level 5 administration skills. In **Table 1**, by way of a non-limiting example, the role of "SysAdmin" is met by "Donna", but only between October 14, 2002 –

October 25, 2002 or November 14, 2002 – November 25, 2002, or by a principal that satisfies the "SystemAdministrator" segment.

In one embodiment, a segment can be persisted in Extensible Markup Language (XML). XML is a platform independent language for representing structured documents. Retrieving information stored in an XML document can be time consuming since the text comprising the XML document must be parsed. To save time, in another embodiment once a XML document representing a segment has been parsed, the information extracted therefrom can be cached to avoid the need to parse the file again.

Figure 2 is the exemplary hierarchy of **Figure 1** further illustrating roles and security policies. Roles are designated by the letter 'R' followed by a parenthetical list of one or more roles. Likewise, policies are designated by the letter 'P' followed by a parenthetical list including a set of roles and an optional capability to which the policy applies. If no capability is present, the policy applies to the resource as a whole. In one embodiment, roles can be considered global in scope or can be associated with a particular resource. A global role is considered within the scope of any resource. In one embodiment, a role associated with a resource is within the scope of that resource. In another embodiment, the role is within the scope of the resource and all of its descendents. In yet another embodiment, the role is within the scope of the resource and all of its descendents unless a role with the same name is associated with a descendent. In this way, a "more local" role occludes a "less local" role of the name.

In **Figure 2**, the role *Anonymous* is associated with the resource *Web App 1*. In one embodiment, *Anonymous* is within the scope of *Web App 1* and all resources beneath it in the hierarchy. Role *G* is associated with resource *Desktop A* and as such, is within the scope of *Desktop A* and its descendents. Role *S* is associated with resource *Page A*. Since *Page A* has no children (i.e., the attribute *Cap 3* does not count as a child), the scope of role *S* is limited to *Page A*. Resource *Booklet 2* is associated with roles *T* and *U*. In one

embodiment, role *T* is within the scope of *Booklet 2* and all of its descendents but the same does not hold true for role *U*. Since a descendent of *Booklet 2* (i.e., *Page Y*) is associated with another role by the same name, the role *U* associated with *Booklet 2* is only within the scope of *Booklet 2* and *Page X*. In one embodiment, the role *U* associated with *Page Y* however is within the scope of all of the descendents of *Page Y* (i.e., *Portlet A, Portlet B,* and *Portlet C*). Roles *V* and *W* are within the scope of *Portlet A*.

In one embodiment, a security policy (hereinafter referred to as a "policy") is an association between a resource, a set of roles, and an optional capability. Generally speaking, a policy grants access to the resource for all principals for which the set of roles evaluates to true. In one embodiment, a policy is satisfied if any of its roles evaluate to true for a given principal. In another embodiment, a policy is satisfied if all of its roles evaluate to true for a given principal. In another embodiment, a security policy integrity system can prevent removing or deleting roles that have policies which depend on them. Although one of skill in the art will recognize that there are many ways to implement such a system, one approach would be to keep track of the number of policies that depend on a particular role by using a reference count. Only when the reference count is equal to zero will the particular role be eligible for removal.

In yet a further embodiment, a policy's set of roles can be an expression including Boolean operators, set operators and roles for operands. A policy can be expressed as the tuple *<resource, roles, [capability]>*, wherein *resource* specifies the name of a resource and *roles* specifies a set of roles, and *capability* is an optional capability. While a policy is predicated on one or more roles, roles are predicated on users and groups. Therefore, one of skill in the art will appreciate that policies are in essence predicated on users, groups, and/or segments. By way of illustration, there are four policies illustrated in **Figure 2**:

P_1 = <Web App 1, {Anonymous}>

P_2 = <Web App 1/Portal 1/Desktop A/Page 2, {G}>

P_3 = <Web App 1/…/Page Y/Portlet A, {W, T}, Cap 1>

P_4 = <Web App 1/…/Page Y/Portlet A, {U, G, Anonymous}, Cap 2>

By way of a non-limiting illustration, assume a principal *p* attempts to access resource *Cap 1*. In order to do so, the security policy P_3 on *Cap 1* requires that *p* satisfy either role *W* or *T*. In one embodiment, all roles within the scope of *Cap 1* (i.e., *Anonymous, G, T, U, U, V,* and *W*) are determined for *p*. If any of the roles that *p* satisfies match *W* or *T*, P_3 is likewise satisfied and access to *Cap 1* is granted for *p*.

By way of a further non-limiting illustration, assume principal *p* attempts to access capability *Cap 2* for resource *Portlet A*. In order to do so, the security policy P_4 on *Cap 2* requires that *p* satisfy one of the roles *U, G* or *Anonymous*. In one embodiment, all roles within the scope of *Portlet A* (i.e., *Anonymous, G, T, U, V* and *W*) are determined for *p*. Note that in one embodiment, the role *U* associated with resource *Booklet 2* is not in the scope of *Portal A*. Instead, the role having the same name but associated with the more "local" resource *Page Y* occludes it. Thus, if any of the roles that *p* satisfies match *U, G* or *Anonymous*, P_4 is satisfied and access to *Cap 2* is granted for *p*. However, since in one embodiment every principal satisfies the role *Anonymous*, P_4 will always be satisfied.

By way of a further non-limiting example, assume *p* attempts to access capability *Cap 4* associated with resource *Booklet 2*. This resource has no policy. In one embodiment, access will be denied. In another embodiment, access will be granted. In yet a further embodiment, access will be granted if *p* satisfies a policy in a parent resource of *Booklet 2*. **Table 2** is a non-limiting illustration of a parent policy search using the resource hierarchy of **Figure 2**. It is important to note, however, that the particular search order or the method of searching is irrelevant for purposes of this disclosure. In yet another embodiment, a resource without an explicit policy can include information regarding its parent policy and thus circumvent the need for a search.

SEARCH STEP	CURRENT RESOURCE	CAPABILITY	POLICY FOUND?
1	Web App 1/Portal 1/Desktop A/Page 2/Booklet 1/Booklet 2	Cap 4	No
2	Web App 1/Portal 1/Desktop A/Page 2/Booklet 1/Booklet 2		No
3	Web App 1/Portal 1/Desktop A/Page 2/Booklet 1	Cap 4	No
4	Web App 1/Portal 1/Desktop A/Page 2/Booklet 1		No
5	Web App 1/Portal 1/Desktop A/Page 2	Cap 4	No
6	Web App 1/Portal 1/Desktop A/Page 2		Yes

Table 2: Exemplary Policy Search

In one embodiment, the search for a policy proceeds as follows. The starting point for the search is the resource that owns the capability (i.e., *Booklet 2*) to which the principal is attempting to access (i.e., *Cap 4*). This is the current resource. If no policy exists at the current resource for the specific capability, in Step 2 we determine whether or not there is a policy merely on the resource itself. If no policy is found, in Step 3 the current resource is set equal to its parent (i.e., *Booklet 1*). If the current resource has no policy for *Cap 4*, we determine whether or not there is a policy on *Booklet 1* itself. If no policy is found, in Step 5 the current resource is set equal to its parent (i.e., *Page 2*). If no policy is found for *Cap 4* at the current resource, we determine in Step 6 whether or not there is a policy on *Page 2* itself. Since this is the case, the search stops at Step 6. *Web App 1/Portal 1/Desktop A/Page 2* has policy P_2. Therefore if *p* satisfies role *G*, access to *Cap 4* is granted for *p*.

In another embodiment, capabilities are associated with particular resource types. For example, booklets may have a type of capability (e.g., *Cap 4*) that is not compatible with or available for other resource types (e.g., pages or desktops). Therefore, when searching for a policy as in **Table 2**, if a

capability is not compatible for the current resource, that resource can be omitted from the search. In yet a further embodiment, if a policy is not found for a given resource type, a global library could be consulted to determine if there are any applicable global policies.

In another embodiment, roles and policies can reside in their own hierarchies, apart from the primary resource hierarchy. For applications that do not need to associate roles and/or policies with resources in the primary hierarchy, such an approach can allow for a shallow role and/or policy tree, perhaps only with a single level. Searching smaller hierarchies can potentially reduce the time it takes to find all roles within scope and locate a policy.

Figure 3 is a diagram of an authorization system in accordance to one embodiment of the invention. Although this diagram depicts objects as functionally separate, such depiction is merely for illustrative purposes. It will be apparent to those skilled in the art that the objects portrayed in **Figure 3** can be arbitrarily combined or divided into separate software, firmware or hardware components. Furthermore, it will also be apparent to those skilled in the art that such components, irregardless of how they are combined or divided, can execute on the same computer or can be arbitrarily distributed among different computers connected by one or more networks.

In one embodiment, security framework **300** is a modular security architecture having a published interface that allows for plug-in components. By way of a non-limiting example, a framework can be a library, a set of interfaces, distributed objects, or any other means for software, firmware and/or hardware components to intercommunicate. Connected to the framework are one or more role mapper components (**302 – 306**). A role mapper maps (e.g., determines which roles are appropriate) a principal to one or more roles based on a resource hierarchy and a context. Each role mapper can implement its own specialized algorithms in this regard and use information and resources beyond that which is provided by the framework. Also connected to the framework are one or more authorizers (**308 – 310**). An authorizer is responsible for

determining if access to a resource can be granted based on whether a principal satisfies a resource policy. Each authorizer can implement its own specialized algorithms in this regard and use information and resources beyond that which is provided by the framework. Finally, adjudicator **314** resolves any difference in outcome between authorization modules and returns a final result (e.g., "grant", "deny" or "abstain"). In one embodiment, the adjudicator can take the logical "or" of the final results such that if any result is a "grant", the outcome of adjudication is "grant". In another embodiment, the adjudicator can take the logical "and" of the final results such that if any result is a "deny", the outcome of adjudication is "deny". In yet a further embodiment, the adjudicator can use a weighted average or other statistical means to determine the final outcome.

A process can interact with the framework in a number of ways which will be apparent to those skilled in the art. In one embodiment, a calling process provides a resource access request ① to the framework **300**. This request can include information about the principal, the resource to which access is requested, and any context information. In another embodiment, the request can contain references to this information. This information is then provided to one or more role mappers ② by the framework. Each role mapper determines which roles are appropriate for the principal based on their own criteria. In another embodiment, each role mapper can implement a cache to speed up searching for roles. Rather than traversing a resource tree to find all roles within scope, each role mapper can cache roles that were previously retrieved from a resource tree based on a key comprising the resource to which access is requested and the principal. After the initial retrieval from a resource tree, subsequent roles for a given resource-principal combination can be taken directly from the cache.

A set of satisfied roles is then returned to the framework in ③. The framework can provide the information from ① and ③ to the authorizer modules in ④. The authorization modules individually determine whether or not a policy is satisfied based on this information and their own criteria. In

another embodiment, each authorizer can implement a cache to speed up searching for policies. Rather than traversing a resource tree to find a policy within scope, each authorizer can cache policies that were previously retrieved from a resource tree based on a key comprising the resource to which access is requested and the principal. After the initial retrieval from a resource tree, subsequent policies for a given resource-principal combination can be taken directly from the cache. The authorizer results (e.g., in terms of grant or deny decisions) are provided to the framework in ⑤ and provided to the adjudicator in ⑥. The adjudicator makes a final decision which it provides to the framework in ⑦. The framework then provides this decision to the calling process in ⑧.

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. Delegated administration allows a hierarchy of roles to manage administrative capabilities. By way of a non-limiting example, administrative capabilities can include the ability to manage customer accounts, the ability to delegate administrative capabilities, the ability to customize or personalize user interface elements (e.g., portals, booklets, desktops, portlets, etc.), the ability to perform administration of an enterprise application, etc. In another embodiment, any capability or property can be delegated. In one embodiment, delegation is an act whereby a principal in one role enables another hierarchically inferior role to have an administrative capability and/or further delegate an administrative capability. In one embodiment, a delegation role is identical to a role and can thusly be defined using predicates (e.g., user, group, currentDate, segment, etc.).

Figure 4 is an illustration of a delegation role hierarchy in accordance to one embodiment of the invention. In one embodiment, delegation roles can be organized into a delegation hierarchy to control the extent of delegation. In one embodiment, delegation roles can be associated with a single top-level resource,

such as an enterprise application, and a delegation role hierarchy can be maintained separate from the resource hierarchy. A security policy can be associated with the enterprise application to limit which principals are allowed to alter the role definitions and the separately maintained role hierarchy. In another embodiment, a fictitious resource hierarchy that mirrors an arbitrary delegation role hierarchy can be utilized whereby each delegation role is associated with a resource corresponding to the delegation role's proper position in the hierarchy. A security policy can be associated with each resource to control which principals can modify the associated role. A security policy at the root of the hierarchy could limit which principals are allowed to modify the fictitious hierarchy itself.

Referring again to **Figure 4**, role *Admin_Role* is at the top of the delegation role hierarchy. In one embodiment, the principal in this role has no limitations in its administrative capabilities or delegation authority. By way of a non-limiting example, a principal in the *Admin_Role* can modify the definition of delegation roles and the delegation hierarchy. In one embodiment, a principal in a delegation role can delegate administrative capabilities only to roles beneath it in a delegation hierarchy. *Admin_Role* has two children, *A_Role* and *B_Role*. *A_Role* has one child, *C_Role*, which as two children: *D_Role* and *E_Role*. By way of a non-limiting example, *Admin_Role* can delegate to all other roles beneath it in the hierarchy. Likewise, *A_Role* can delegate to *C_Role*, *D_Role* and *E_Role*. Whereas *C_Role* can only delegate to *D_Role* and *E_Role*. The leaves of the tree, *D_Role*, *E_Role* and *B_Role* cannot delegate since they have no children. In another embodiment, a node in the hierarchy can be related to more than one parent. This allows more than one superior role to delegate to an inferior role.

In one embodiment, a delegation can be represented by a security policy. The policy is associated with a delegated resource/capability and is based on the role to which the resource/capability was delegated. **Figure 5** is an illustration of exemplary delegation security policies in one embodiment of the invention.

Assume for this example that the delegation hierarchy of **Figure 4** holds. Notice that the root resource in **Figure 5**, *Enterprise App 1* is associated with the following roles: *Admin_Role, A_Role, B_Role, C_Role, D_Role* and *E_Role*. The hierarchy depicted in **Figure 5** could include other resources, roles and policies, but is limited for illustrative purposes. In one embodiment, a delegation creates a policy on the resource who's capability is being delegated. For example, resource *Web App 1* has an *Admin* capability and an associated security policy *P(D_Role)*. A principal in the role of *C_Role, A_Role* or *Admin_Role* created this policy by delegating to *D_Role* the *Admin* capability for *Web App 1*. (It will be apparent to those of skill in the art that any capability can be delegated; i.e., not just *Admin.*) Thus, principals that satisfy *D_Role* can perform administration of *Web App 1*. However, since *Web App 1* does not have a delegation capability, a principal satisfying the *D_Role* cannot further delegate *Web App 1*'s *Admin* capability.

Resource *Desktop A* has two capabilities, *Admin* and *Delegate*, each of which has a policy. The policy *P(A_Role)*attached to both indicates that a principal in the role of *Admin_Role* delegated to *Role_A* the capability to both administer *Desktop A* and further delegate this capability. Thus, a principal in *Role_A* can further delegate both the *Admin* and *Delegate* capabilities to hierarchically inferior delegation roles (i.e., *C_Role, D_Role* and *E_Role*). For example, resource *Desktop B* has a capability *Admin* that has a policy *P(C_Role)*. This policy was put in place by a principal in the role of *A_Role* or *Admin_Role*. A principal in the role of *C_Role* will be able to administer *Desktop B*, but will not be able to further delegate this capability.

In one embodiment, a delegation to a node that is already delegated to by a principal in a hierarchically superior delegation role is not permitted. Referring to Figures 4 and 5, and by way of a non-limiting illustration, if resource *Portal 2* had a policy *P(A_Role)*, a principal in the role of *C_Role* would not be able to delegate *Portal 2* since it had been delegated to a role superior to *C_Role* (i.e., *A_Role*).

In another embodiment, aspects of user group administration can be delegated. By way of a non-limiting example, user groups can by organized into a hierarchy by viewing them as children of an enterprise application resource. Capabilities that can be delegated include: user profile administration, the ability to view the members of group, and the ability to create, update and remove users and groups.

One embodiment may be implemented using a conventional general purpose or a specialized digital computer or microprocessor(s) programmed according to the teachings of the present disclosure, as will be apparent to those skilled in the computer art. Appropriate software coding can readily be prepared by skilled programmers based on the teachings of the present disclosure, as will be apparent to those skilled in the software art. The invention may also be implemented by the preparation of integrated circuits or by interconnecting an appropriate network of conventional component circuits, as will be readily apparent to those skilled in the art.

One embodiment includes a computer program product which is a storage medium (media) having instructions stored thereon/in which can be used to program a computer to perform any of the features presented herein. The storage medium can include, but is not limited to, any type of disk including floppy disks, optical discs, DVD, CD-ROMs, microdrive, and magneto-optical disks, ROMs, RAMs, EPROMs, EEPROMs, DRAMs, VRAMs, flash memory devices, magnetic or optical cards, nanosystems (including molecular memory ICs), or any type of media or device suitable for storing instructions and/or data.

Stored on any one of the computer readable medium (media), the present invention includes software for controlling both the hardware of the general purpose/specialized computer or microprocessor, and for enabling the computer or microprocessor to interact with a human user or other mechanism utilizing the results of the present invention. Such software may include, but is not limited to, device drivers, operating systems, execution environments/

containers, and user applications.

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.

CLAIMS

What is claimed is:

1. A method for adaptively managing entitlements, comprising the steps of:

providing for the association of a role with a first resource; and

providing for the association of a policy with a second resource, wherein the policy is based at least partially on the role; and

providing for hierarchically relating the role and the policy; and

wherein the role is hierarchically equal or superior to the policy.

2. The method of claim 1 wherein:

the step of providing for the association of the policy with the second resource is initiated by an authenticated user, group or process.

3. The method of claim 1 including the step of:

providing for mapping the role to a principal in order to specify whether or not the principal can access the second resource.

4. The method of claim 1 including the step of:

providing for evaluating the role to true or false for a principal in a context.

5. The method of claim 1 wherein:

the role is a Boolean expression that can include at least one of (1) another Boolean expression and (2) a predicate.

6. The method of claim 5 wherein:

the predicate is one of user, group, time and segment.

7. The method of claim 5 wherein:

the predicate can be evaluated against a principal and a context.

8. The method of claim 5 wherein:

the predicate is a segment that can be specified in plain language.

9. The method of claim 1 wherein:

the policy is an association between the second resource and a set of roles.

10. The method of claim 1 wherein:

the first resource and the second resource are part of an enterprise application.

11. A method for adaptively managing entitlements in an enterprise application, comprising the steps of:

providing for the association of a role with a first enterprise application resource;

providing for the association of a policy with a second enterprise application resource, wherein the policy is based at least partially on the role;

providing for mapping the role to a principal in order to specify whether or not the principal can access the second resource;

providing for hierarchically relating the role and the policy; and

wherein the role is hierarchically equal or superior to the policy.

12. The method of claim 11 wherein:

the step of providing for the association of the policy with the second resource is initiated by an authenticated user, group or process.

13. The method of claim 11 wherein:

the role can supercede a second role associated with a parent of the first

resource; and

wherein the first policy can supercede a second policy associated with a parent of the second resource.

14. The method of claim 11 including the step of:

providing for evaluating the role to true or false for a principal in a context.

15. The method of claim 11 wherein:

the role is a Boolean expression that can include at least one of (1) another Boolean expression and (2) a predicate.

16. The method of claim 15 wherein:

the predicate is one of user, group, time and segment.

17. The method of claim 15 wherein:

the predicate can be evaluated against a principal and a context.

18. The method of claim 15 wherein:

the predicate is a segment that can be specified in plain language.

19. The method of claim 11 wherein:

the policy is an association between the second resource and a set of roles.

20. A method adapted for managing entitlements, comprising the steps of:

providing for the association of a first role with a first resource in a hierarchy of resources;

providing for the association of a first policy with a second resource in the hierarchy of resources, wherein the first policy is based at least partially on

the first role; and

wherein the first role can supercede a second role associated with a parent of the first resource if the first role and the second role have the same identity; and

wherein the first policy can supercede a second policy associated with a parent of the second resource if the first policy and the second policy have the same identity.

21. The method of claim 20 wherein:

the step of providing for the association of the first policy with the second resource is initiated by an authenticated user, group or process.

22. The method of claim 20 including the step of:

providing for mapping the first role to a principal in order to specify whether or not the principal can access the second resource.

23. The method of claim 20 including the step of:

providing for evaluating the first role to true or false for a principal in a context.

24. The method of claim 20 wherein:

the first role is a Boolean expression that can include at least one of (1) another Boolean expression and (2) a predicate.

25. The method of claim 24 wherein:

the predicate is one of user, group, time and segment.

26. The method of claim 24 wherein:

the predicate can be evaluated against a principal and a context.

27. The method of claim 24 wherein:

the predicate is a segment that can be specified in plain language.

28. The method of claim 20 wherein:

the first policy is an association between the second resource and a set of roles.

29. The method of claim 20 wherein:

the first resource and the second resource are part of an enterprise application.

30. A method adapted for managing entitlements, comprising the steps of:

providing for the association of a role with a first resource in a hierarchy of resources;

providing for the association of a policy with a second resource in the hierarchy of resources, wherein the policy is based at least partially on the role; and

wherein the role blocks a less local role; and

wherein the policy blocks a less local policy.

31. The method of claim 30 wherein:

the step of providing for the association of the policy with the second resource is initiated by an authenticated user, group or process.

32. The method of claim 30 including the step of:

providing for mapping the role to a principal in order to specify whether or not the principal can access the second resource.

33. The method of claim 30 including the step of:

providing for evaluating the role to true or false for a principal in a

context.

34. The method of claim 30 wherein:

the role is a Boolean expression that can include at least one of (1) another Boolean expression and (2) a predicate.

35. The method of claim 34 wherein:

the predicate is one of user, group, time and segment.

36. The method of claim 34 wherein:

the predicate can be evaluated against a principal and a context.

37. The method of claim 34 wherein:

the predicate is a segment that can be specified in plain language.

38. The method of claim 30 wherein:

the policy is an association between the second resource and a set of roles.

39. The method of claim 30 wherein:

the first resource and the second resource are part of an enterprise application.

40. A method adapted for managing entitlements, comprising the steps of:

providing for the association of a role with a first resource in a hierarchy of resources;

providing for the association of a policy with a second resource in the hierarchy of resources, wherein the policy is based at least partially on the role; and

wherein the role blocks a less local role.

41. The method of claim 40 wherein:
the policy blocks a less local policy.

42. The method of claim 40 wherein:
the step of providing for the association of the policy with the second resource is initiated by an authenticated user, group or process.

43. The method of claim 40 including the step of:
providing for mapping the role to a principal in order to specify whether or not the principal can access the second resource.

44. The method of claim 40 including the step of:
providing for evaluating the role to true or false for a principal in a context.

45. The method of claim 40 wherein:
the role is a Boolean expression that can include at least one of (1) another Boolean expression and (2) a predicate.

46. The method of claim 45 wherein:
the predicate is one of user, group, time and segment.

47. The method of claim 45 wherein:
the predicate can be evaluated against a principal and a context.

48. The method of claim 45 wherein:
the predicate is a segment that can be specified in plain language.

49. The method of claim 40 wherein:

the policy is an association between the second resource and a set of roles.

50. The method of claim 40 wherein:

the first resource and the second resource are part of an enterprise application.

51. A computer data signal embodied in a transmission medium, comprising:

a code segment including instructions for:

associating a role with a first resource; and

associating a policy with a second resource, wherein the policy is based partially on the role; and

hierarchically relating the role and the policy; and

wherein the role is hierarchically equal or superior to the policy.

52. The computer data signal of claim 51 wherein:

the step of providing for the association of the policy with the second resource is initiated by an authenticated user, group or process.

53. The computer data signal of claim 51 including the step of:

providing for mapping the role to a principal in order to specify whether or not the principal can access the second resource.

54. The computer data signal of claim 51 including the step of:

providing for evaluating the role to true or false for a principal in a context.

55. The computer data signal of claim 51 wherein:

the role is a Boolean expression that can include at least one of (1)

another Boolean expression and (2) a predicate.

56. The computer data signal of claim 55 wherein:
the predicate is one of user, group, time and segment.

57. The computer data signal of claim 55 wherein:
the predicate can be evaluated against a principal and a context.

58. The computer data signal of claim 55 wherein:
the predicate is a segment that can be specified in plain language.

59. The computer data signal of claim 51 wherein:
the policy is an association between the second resource and a set of roles.

60. The computer data signal of claim 51 wherein:
the first resource and the second resource are part of an enterprise application.

61. A memory for storing data to be accessed by an application program being executed on a data processing system, comprising:
a data structure stored in the memory, the data structure including:
an object adapted for representing at least one resource and adapted to be connected to at least one other like object to represent a hierarchy of resources; and
wherein the object and the at least one other like object can be associated with at least one of (a) a security policy and (b) a role such that a hierarchy of security policies and roles is established.

62. The memory of claim 61 wherein:

a hierarchically inferior security policy supercedes a hierarchically superior security policy.

63. The memory of claim 61 wherein:
a hierarchically inferior role supercedes a hierarchically superior role.

64. The memory of claim 61 wherein:
the at least one role evaluates to true or false for a principal in a context.

65. The memory of claim 61 wherein:
the at least one role is a Boolean expression that can include at least one of (1) another Boolean expression and a (2) predicate.

66. The memory of claim 65 wherein:
the predicate is one of user, group, time and segment.

67. The memory of claim 65 wherein:
the predicate can be evaluated against a principal and a context.

68. The memory of claim 65 wherein:
the predicate is a segment that can be specified in plain language.

69. The memory of claim 61 wherein:
a security policy is an association between an object and a set of roles.

70. A machine readable medium having instructions stored thereon that when executed by a processor cause a system to:
provide for the association of a role with a first resource; and
provide for the association of a policy with a second resource, wherein the policy is based at least partially on the role; and

provide for hierarchically relating the role and the policy; and

wherein the role is hierarchically equal or superior to the policy.

71. The machine readable medium of claim 70 wherein:

providing for the association of the policy with the second resource is initiated by an authenticated user, group or process.

72. The machine readable medium of claim 70 including instructions which when executed by a processor cause the system to:

provide for mapping the role to a principal in order to specify whether or not the principal can access the second resource.

73. The machine readable medium of claim 70 including instructions which when executed by a processor cause the system to:

provide for evaluating the role to true or false for a principal in a context.

74. The machine readable medium of claim 70 wherein:

the role is a Boolean expression that can include at least one of (1) another Boolean expression and (2) a predicate.

75. The machine readable medium of claim 74 wherein:

the predicate is one of user, group, time and segment.

76. The machine readable medium of claim 74 wherein:

the predicate can be evaluated against a principal and a context.

77. The machine readable medium of claim 74 wherein:

the predicate is a segment that can be specified in plain language.

78. The machine readable medium of claim 70 wherein:

the policy is an association between the second resource and a set of roles.

79. The machine readable medium of claim 70 wherein:

the first resource and the second resource are part of an enterprise application.

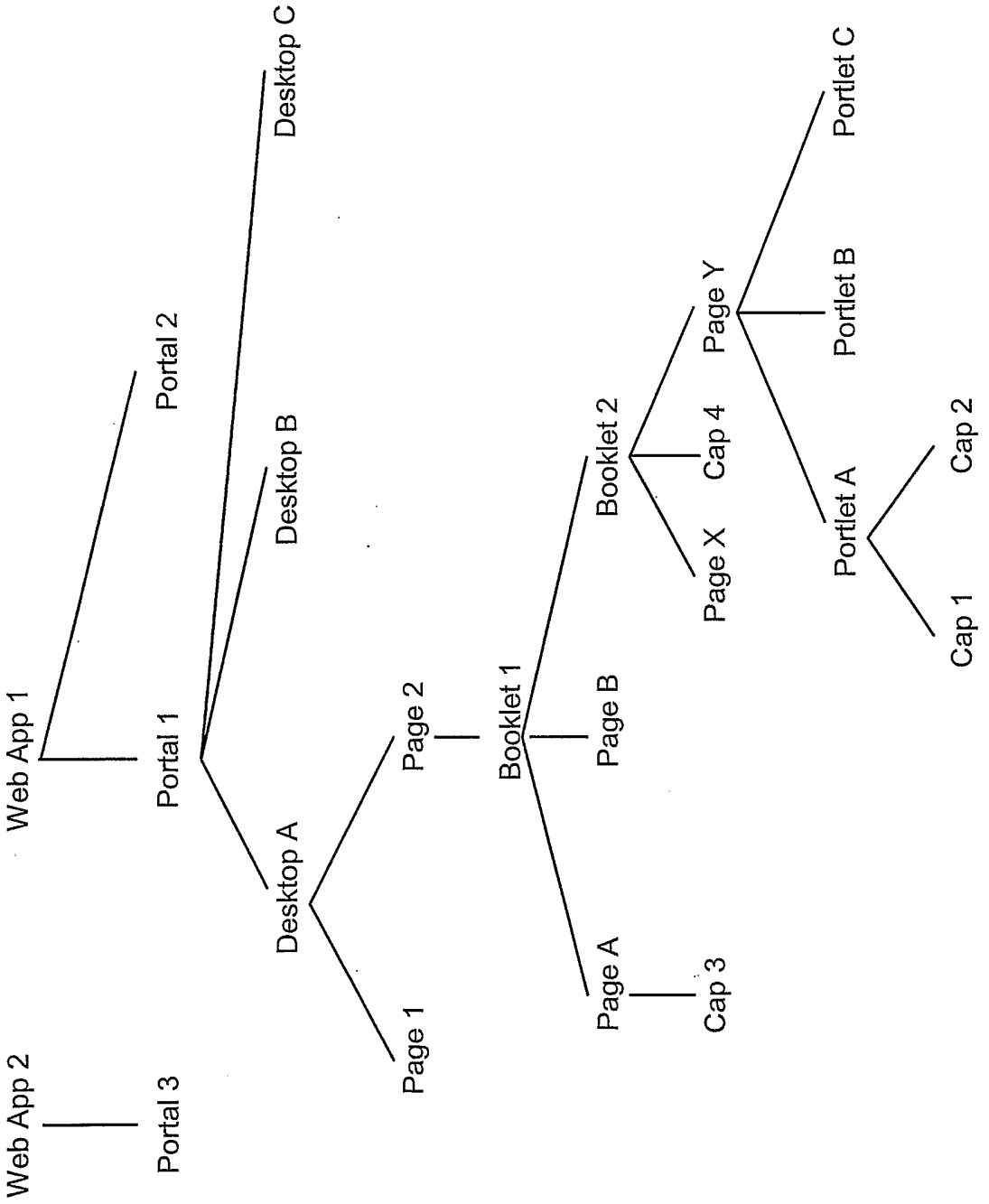

Web App 1
Web App 2
Portal 1
Portal 2
Portal 3
Desktop A
Desktop B
Desktop C
Page 1
Page 2
Booklet 1
Page A
Page B
Booklet 2
Cap 3
Page X
Cap 4
Page Y
Portlet A
Portlet B
Portlet C
Cap 1
Cap 2

Figure 1

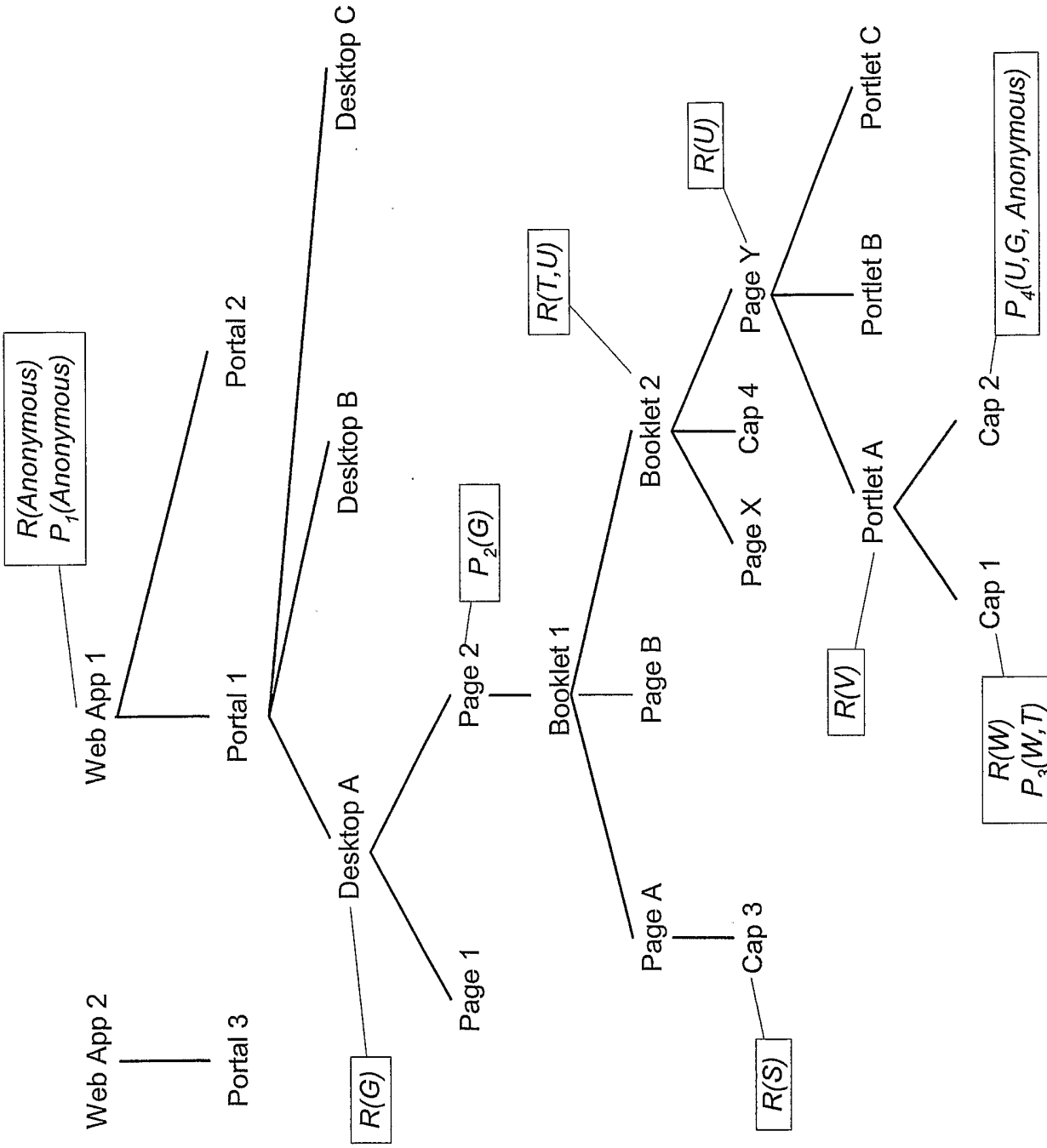

R(Anonymous)
P1(Anonymous)
Web App 1
Portal 1
Portal 2
Desktop A
Desktop B
Desktop C
R(G)
Page 1
Page 2
P2(G)
Booklet 1
Page A
Page B
Booklet 2
R(T,U)
Cap 3
R(S)
Page X
Cap 4
Page Y
R(U)
R(V)
Portlet A
Portlet B
Portlet C
Cap 1
Cap 2
R(W)
P3(W,T)
P4(U,G, Anonymous)
Web App 2
Portal 3

Figure 2

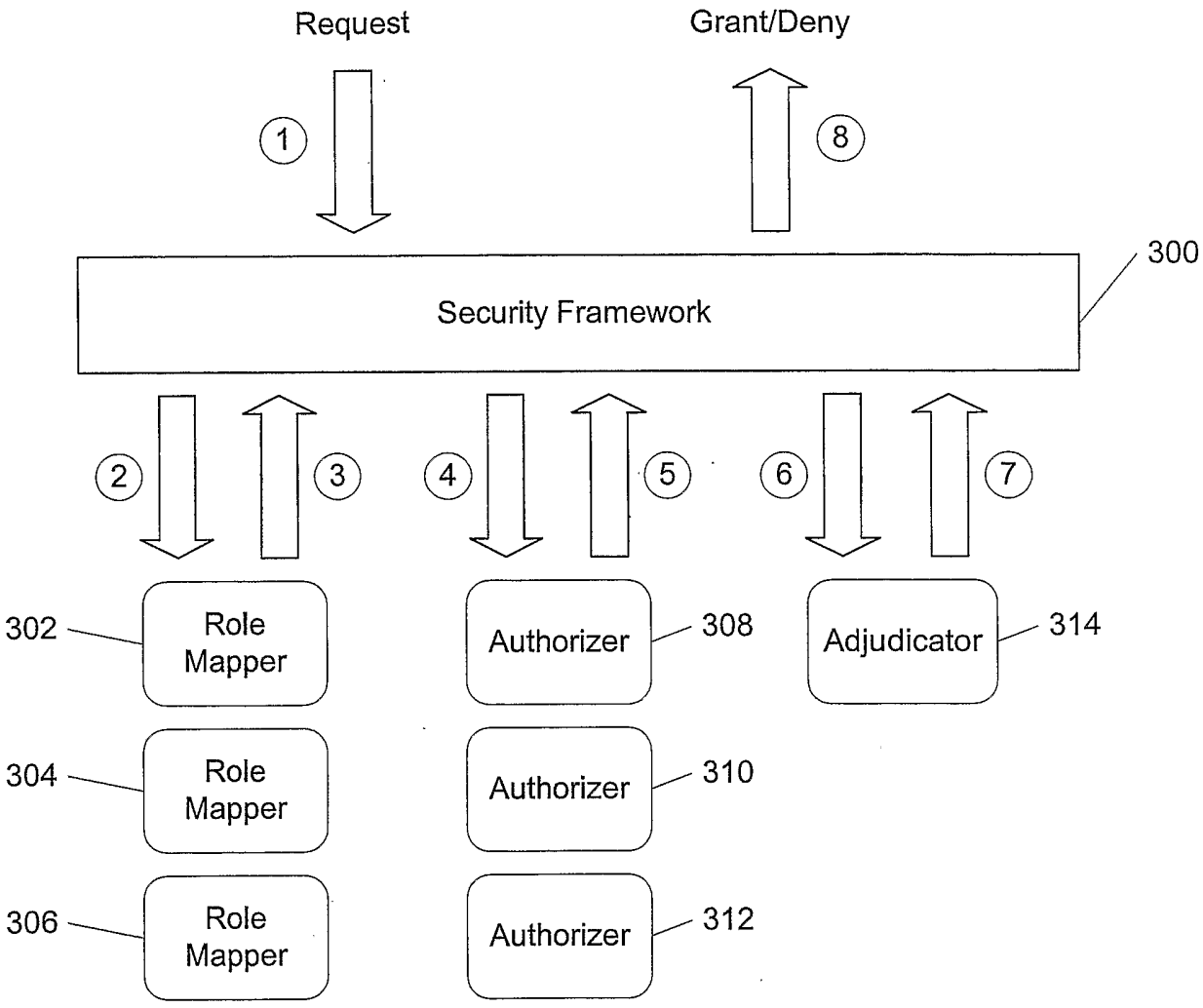

Request
Grant/Deny
1
8
300
Security Framework
2
3
4
5
6
7
302
Role Mapper
304
Role Mapper
306
Role Mapper
Authorizer
308
Authorizer
310
Authorizer
312
Adjudicator
314

Figure 3

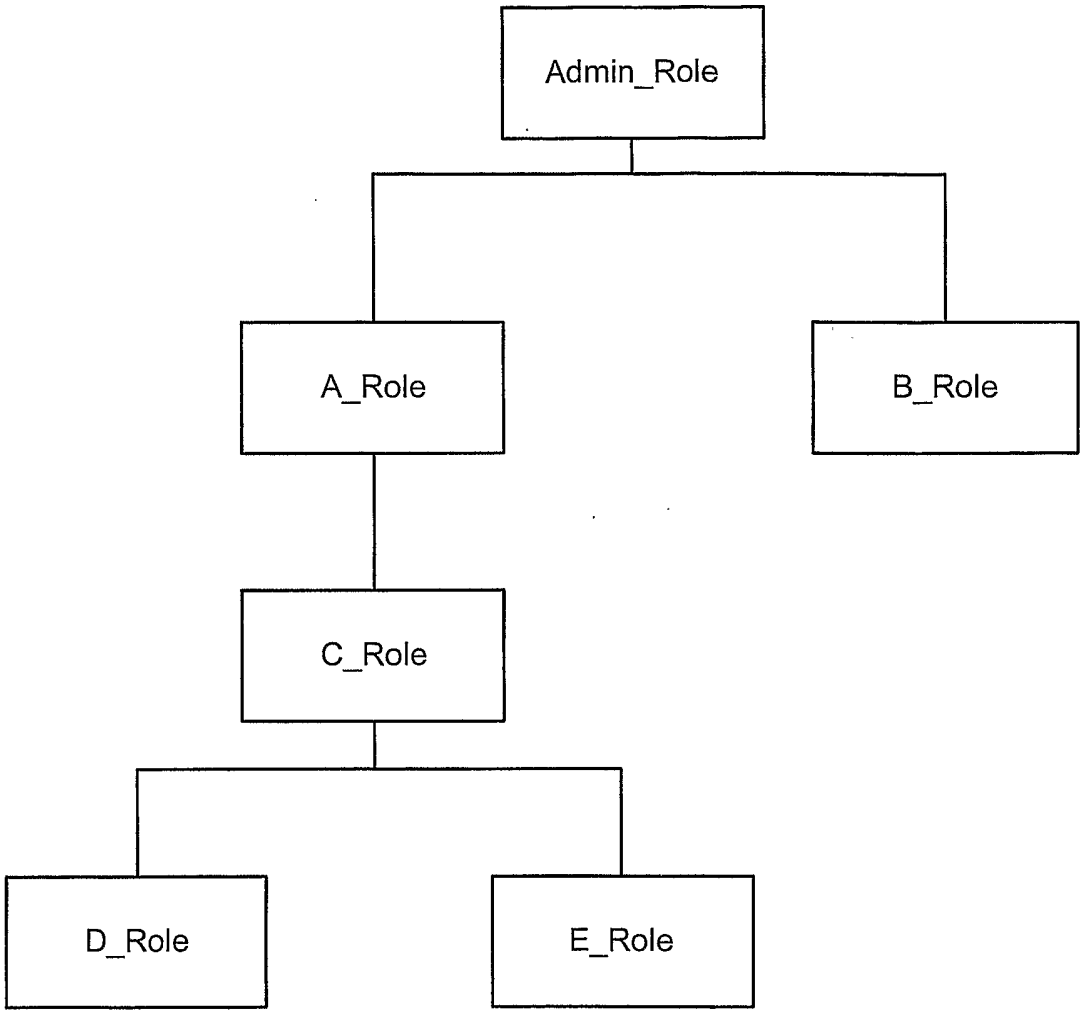


Figure 4

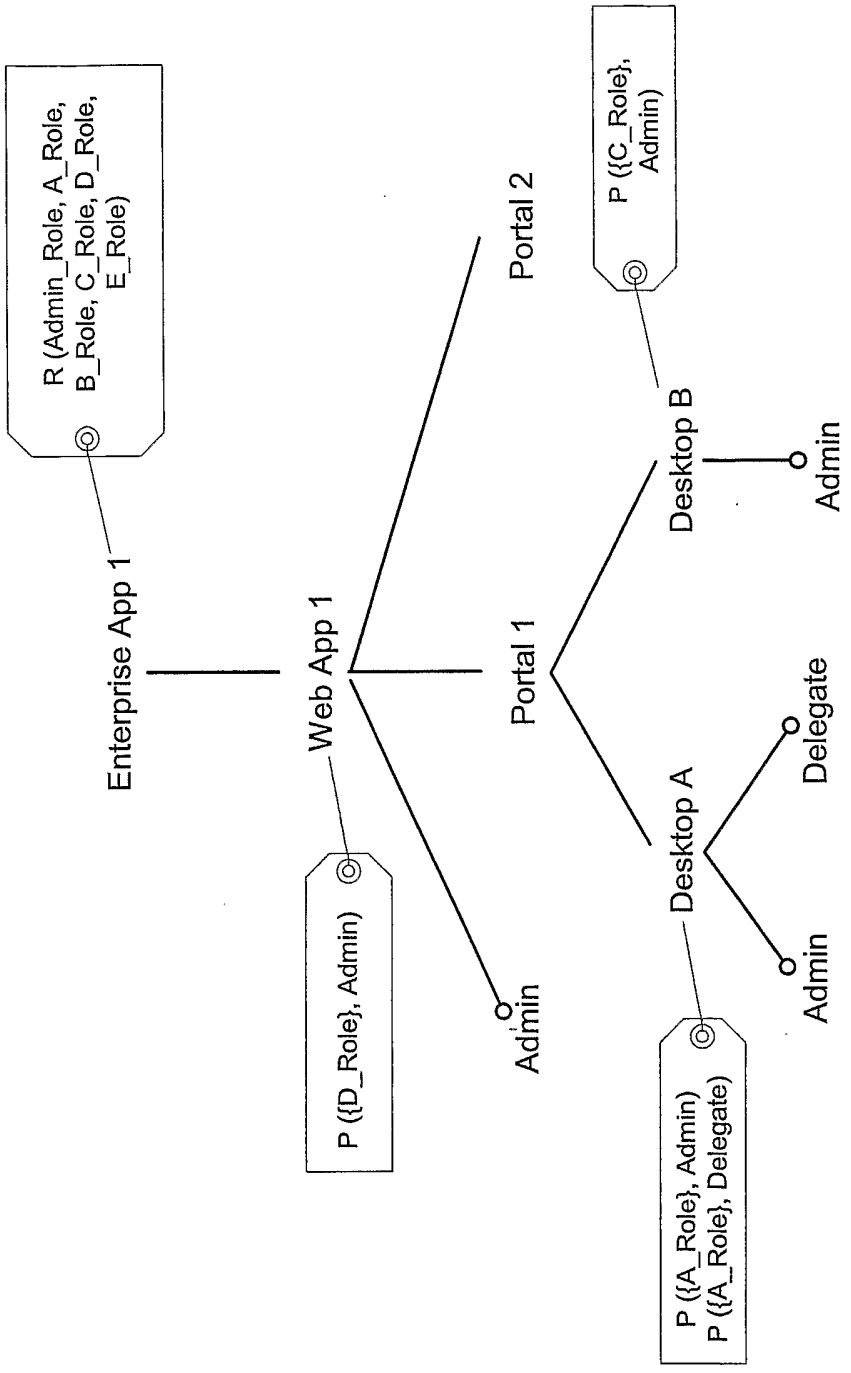

R (Admin_Role, A_Role, B_Role, C_Role, D_Role, E_Role)
Enterprise App 1
Web App 1
P ({D_Role}, Admin)
Admin
Portal 1
Portal 2
P ({C_Role}, Admin)
Desktop B
Admin
Desktop A
Delegate
Admin
P ({A_Role}, Admin)
P ({A_Role}, Delegate)

Figure 5