

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
15 January 2009 (15.01.2009)

PCT

(10) International Publication Number
WO 2009/008567 A1

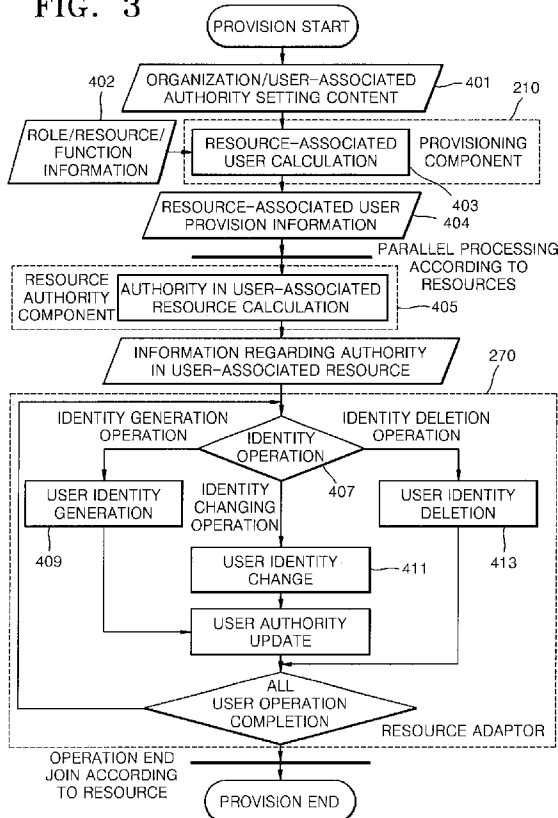
- (51) International Patent Classification:
G06F 15/00 (2006.01)
- (21) International Application Number:
PCT/KR2007/003594
- (22) International Filing Date: 26 July 2007 (26.07.2007)
- (25) Filing Language: Korean
- (26) Publication Language: English
- (30) Priority Data:
10-2007-0068773 9 July 2007 (09.07.2007) KR
- (71) Applicant (for all designated States except US): NETS CO., LTD. [KR/KR]; 6th Floor., Jungang Bldg. 161-15, Samseong-dong, Gangnam-gu, Seoul 135-090 (KR).
- (72) Inventor; and
- (75) Inventor/Applicant (for US only): MOON, Sung Kwang [KR/KR]; 101-702 Doosan Weve Apt., Guro3-dong, Guro-gu, Seoul 152-053 (KR).

- (74) Agent: Y.P. LEE, MOCK & PARTNERS; 1575-1 Seocho-dong, Seocho-gu, Seoul 137-875 (KR).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— with international search report

(54) Title: PROVISIONING APPARATUS FOR RESOURCES AND AUTHORITIES FOR INTEGRATED IDENTITY MANAGEMENT

FIG. 3



(57) Abstract: Provided is a resource provisioning apparatus in identity management. More specifically, provided is an apparatus for managing a resource as an authority and provisioning a resource identity and a resource authority according to the authority in an integrated identity management technology. Using a method according to an embodiment of the present invention, customers can have the following advantages. 1) A function and a role in a resource can be defined. 2) A role including a resource can be defined as a shared role. 3) An authority (role, resource, function) can be allocated as allowance or rejection to an organization and a user. Accordingly, an authority allocated to a final user can be easily inquired about. 4) The provisioning system can provide an identity according to resources allocated to a final user and provide an authority (function and role) in resources, so that integrated identity and authority management can be implemented in a center.

WO 2009/008567 A1

PROVISIONING APPARATUS FOR RESOURCES AND AUTHORITIES FOR INTEGRATED IDENTITY MANAGEMENT

TECHNICAL FIELD

5 The present invention relates to a resource provisioning apparatus and method of identity management, and more particularly, to an apparatus for performing provisioning of resource identities and resource authorities according to authorities by managing resources as the authorities in an integrated identity management technology.

10

BACKGROUND ART

 The purpose of an identity management field is to automate operations of generating an identity for a resource used by a user and deleting the identity by managing a life cycle of a user identity. In identity management, according to whether
15 or not to use a resource set to a user or a group, an identity is generated in the resource or deleted from the resource.

 The user identity is used in a different way from a general authority when associated with internal organization management. More specifically, in the organization management, authority of a particular user over a particular application or
20 a system is set, and a resource identity provisioning function is required according to the resource authority.

 First, terms used in the description will now be defined.

 Resource represents an application system used by a user or an operating system such as UNIX and refers to a system to be provisioned. Although the
25 application system can have an authority such as a function or a role in an application and the operating system can have an operating system (OS) authority, in general, provisioning is performed on an identity itself.

 Identity means an ID representing a resource-associated user such as a UNIX account, a windows user, and a groupware login ID.

30 Provisioning means automating a life cycle of a resource-associated identity according to a life cycle of a user by generating or deleting identity in or from an associated resource according to whether or not a user can use the resource.

 Authority is a set representing entitlement in the application or the operating

system and is operated as a function or a role that is a set of functions.

A conventional resource identity provisioning method is described as follows. For resource allocation, an existing identity management product uses a direct allocation method or an allocation method according to roles. The direct allocation method means one-to-one mapping between a user or a user's organization/group and resource. The allocation method according to roles means one-to-one mapping between the user or the user's organization/group and a role.

The allocation may use two schemes. More specifically, a scheme for allocating a resource and a role to be used for a user or an organization/group or a scheme for allocating a user or an organization/group to be used for a resource or a role as a filter type may be used. However, the latter has a problem in that resource information used on the basis of users and organizations cannot be obtained.

In existing resource identity provisioning, whether or not the resource is to be used can be set. However, setting whether or not the resource is to be used by using a resource internal authority is impossible. Specifically, setting whether or not the resource is to be used according to whether a detailed function of the resource is used is impossible. In addition, since a role is defined as a set of resources, a role in a resource cannot be expressed.

In addition, in existing resource identity provisioning, resource identity provisioning is possible. However, authority provisioning in the resource is impossible.

DETAILED DESCRIPTION OF THE INVENTION

TECHNICAL PROBLEM

The present invention provides a provisioning apparatus capable of managing a function in a resource and a role that is a set of functions, a resource independent role, and a resource as an authority and provisioning a resource authority in addition to a resource identity based on the authority. More specifically, the present invention also provides a management method of inheriting or rejecting an authority for resource provisioning and an apparatus for resource provisioning by setting an optimal authority.

TECHNICAL SOLUTION

According to an aspect of the present invention, there is provided an authority-based resource identity and authority provisioning apparatus for integrated identity management, comprising: a management application which performs

organization/user authority setting; a provisioning component which calculates resource-associated users by using authority information set by the management application to generate resource-associated user provision information; a resource authority component which performs parallel processing on the generated

5 resource-associated user provision information according to resources to calculate an authority in a resource according to users; and a resource adaptor which performs an identity operation by using information on the calculated authority in a resource according to users, wherein the identity operation includes user identity generation, identity change, and identity deletion, and wherein all user identity operations are

10 performed according to resources.

In the above aspect of the present invention, the authority information set by the management application includes "authority allowance" for users, and "authority allowance inheritance" and "authority rejection inheritance" for organizations. In addition, the management application may include an authority setting user interface

15 which includes authority types (role, resource, and menu or function), a selected authority display, and a resource selection window.

In addition, the provisioning component may use role/resource/menu or function information data in order to generate resource-associated user provision information by calculating resource-associated users. In addition, the provisioning component may

20 have a function of converting an "organization/user/authority management operation" into a "resource-associated identity and authority provisioning operation", obtains information regarding an associated resource to be provisioned to a user from the authority information, and transmits resource-associated operation information to the resource authority component. A resource calculation method used by the

25 provisioning component is as follows.

$$\text{(to-be-provisioned resources)} = \text{(total allowed resources)} - \text{(total rejected resources)}$$

$$\text{(total allowed resources)} = \text{(allowed resources)}$$

$$\cup \text{(resources in an allowed role)}$$

$$\cup \text{(included-in-function resources in an allowed role)}$$

$$\begin{aligned} & \cup \text{ (included-in-allowable-function resources)} \\ \text{(total rejected resources)} &= \text{(rejected resources)} \\ & \cup \text{ (resources in a rejected role)} \\ & \cup \text{ (included-in-function resources in a rejected role)} \\ & \cup \text{ (included-in-rejected-function resources)} \end{aligned}$$

In addition, the resource-associated user calculation may be performed by using:
 a unit which inquires to-be-changed-authority resource associated user information and
 setting the information to a set A; a unit which changing an authority of an organization
 5 and a user; a unit which inquires to-be-changed-authority resource associated user
 information and setting the information to a set B; a unit which deletes identities of
 users who are included in the set A-B and adding the identities to a list, deleting
 identities of users who are included in the set B-A and adding the identities to a list, and
 calculating users who are included in the set $A \cap B$; a unit which determines whether or
 10 not user-associated operation calculation is completed by inquiring individual user
 information; and a unit which determines a user-included set when the operation
 calculation is not completed, and performing resource identity creation and list addition,
 resource identity update and list addition, or resource identity deletion or list addition
 when the user-included set is the set B-A, the set $A \cap B$, or the set A-B, respectively.

15 In addition, the resource-associated user information may be configured as a
 Hashtable including a to-be-processed (added/amended/deleted) user information list
 by using a resource as a key.

In addition, the resource authority component may obtain authority information
 regarding users in the resource according to a predetermined resource authority
 20 calculation method and transmit user identity and authority (role/function) information to
 the resource adaptor, and the resource authority calculation method may be performed
 as follows.

$$\begin{aligned} \text{(resource role)} &= \text{(total allowed roles in allowed resources)} - \text{(total} \\ & \text{rejected roles in allowed resources)} \\ \text{(function)} &= \text{(total allowed functions in allowed resources)} - \text{(total} \\ & \text{rejected functions in allowed resources)} \end{aligned}$$

$$\begin{aligned}
 & \text{(total allowed functions)} = \text{(allowed functions)} \cup \\
 & \text{(functions in allowed roles)} \\
 & \text{(total rejected functions)} = \text{(rejected functions)} \cup \\
 & \text{(functions in rejected roles)}
 \end{aligned}$$

In addition, the resource adaptor may perform generation, change, deletion, and authority synchronization of identities on an associated system by using the identity management operation for the resource obtained by the provisioning component and identity and authority information regarding resources obtained by the resource authority component.

DESCRIPTION OF THE DRAWINGS

FIG. 1 is a view illustrating a data model which represents an authority structure.

FIG. 2 is a schematic flowchart illustrating a provisioning operation according to an embodiment of the present invention.

FIGS. 3 to 6 are flowcharts illustrating a provisioning operation according to an embodiment of the present invention.

FIGS. 7 to 9 are views illustrating examples of a data model used for provisioning according to an embodiment of the present invention.

BEST MODE

<Description of Authority Setting and Allocation as a Premise of the Present Invention>

First, "authority", which is an object of the present invention, is defined. The authority includes a role, a resource, and a function in the resource. The role includes a resource roll that is a set of functions in a resource and a shared role which includes resources and functions.

The authority is set by a combination of the following operations.

1) Authority inheritance: when an authority is set to be inherited by an organization, a subordinate organization or a user thereof receives the authority.

2) Authority allowance and rejection

When an authority is allowed by an organization/user, the user can finally have an inheritance result and a right to use components of the authority. When the

authority for the organization/user is rejected, the user cannot have the inheritance result and the right to use the components of the authority. When the allowance and the rejection are set at the same time for the same role, resource, and function, the rejection has precedence over the allowance.

5 The authority allocation is classified into authority allocation to a group and authority allocation to a user.

1) Authority Allocation to Group

A group is managed in a hierarchical structure or in a flat structure. An organization is the same as the group in the hierarchical structure and can generate a user. A group which is not the organization can only include users.

10 The group is allocated with an authority by using the following operations. (a) Authority allowance: only allocated groups have the authority. (b) Authority allowance inheritance: allocated groups and subordinate groups have the authority. (c) Authority rejection: allocated groups do not have the authority. (d) Authority rejection inheritance: allocated groups and subordinate groups do not have the authority.

15 A user of a group has a final authority. When the same authority is allocated to or inherited by a group as the allowance or the rejection, the group firstly rejects the authority and does not have the authority.

2) Authority Allocation to User

20 A user is a bottom object in an organization structure and directly is included in the organization. Otherwise, the user may be included in several organizations (concurrent positions) or several groups. The user may be allocated with the authority by using the following operations. (a) Authority allowance: only allocated groups have the authority. (b) Authority rejection: allocated groups do not have the authority.

25 The user receives the authority allocated to all organizations and groups, and has directly allocated authority. When the same authority is allocated to or inherited by the user as the allowance or the rejection, the user firstly rejects the authority and does not have the authority.

30 A structure of the authority is classified into an organization structure (using a hierarchical structure and a multiple-group relationship model), an authority structure (using a role, a resource, a function entity, and a member relationship therebetween), and an authority allocation structure (setting (allowing/rejecting) an authority according to groups and users and determining whether to inherit)). An entity-relationship (ER)

diagram of the authority structure is illustrated in FIG. 1.

<Provisioning Flow>

FIG. 2 is a view for explaining a concept of a provisioning method and apparatus according to an embodiment of the present invention. Referring to FIG. 2, by using authority information set by a management application 100, three components (a provisioning component 210, a resource authority component 240, and a resource adaptor 270) of a provisioning system 200 provisions identity/authority information according to resources 300.

The authority information set by the management application 100 is exemplified in FIG. 2. "Authority allowance" is set to a user 140, "authority allowance inheritance" is set to a department 100 in a first level, and "authority rejection inheritance" is set to a department 130 in a third level. A provisioning process of the provisioning system 200 is described with reference to a flowchart illustrated in FIG. 3.

Referring to FIG. 3, when the provisioning is started, the management application 100 performs organization/user-associated authority setting (operation 401). An example of an authority setting display needed for the organization/user authority setting in operation 401 performed by the management application 100 is illustrated in FIG. 4. In FIG. 4, an authority setting user interface (UI) including authority types (role, resource, and menu or function), a selected authority display, and a resource selection window are illustrated.

Next, the provisioning component 210 generates resource-associated user provision information by calculating resource-associated users (operation 403). Here, role, resource, and menu or function information data is used (operation 402). Parallel processing is performed on the generated resource-associated user provision information 404 according to resources so that the resource authority component 240 calculates an authority in a user-associated resource (operation 405).

An identity operation is performed on the calculated authority information in the user-associated resource by the resource adaptor 270 (operation 407).

The identity operation includes user identity generation 409, identity change 411, and identity deletion 413. After all user identity operations are completed for each of the resources, the provisioning is terminated. In the authority information in the user-associated resource, the authority in the resource means an included-in-function

resource and a role that is a set including the included-in-function resources. Only allowed authority information that is finally calculated according to authority granting such as allowance, rejection, and inheritance is obtained. For example, when a user receives 'manager' and 'inspector' authorities, and the inspector authority is allocated as the rejection, since the rejection has precedence over the allowance, the user has only the manager authority. In addition, a user authority in a user authority updating operation means an allowed function and role that is finally calculated from an included-in-function resource and role.

Returning to FIG. 2, the provisioning component 210 has a function of converting an "organization/user/authority management operation" into a "resource-associated identity and authority provisioning operation". According to a resource calculation method, information regarding an associated resource 300 to be provisioned to a user is obtained from the authority information, and resource-associated operation information is transmitted to the resource authority component 240. The resource calculation method is performed as follows. Using the method, the associated resource to be provisioned can be obtained even when only a function is allocated, and a resource of which a function is not defined can be allocated.

$\begin{aligned} &(\text{to-be-provisioned resources}) = (\text{total allowed resources}) - (\text{total rejected resources}) \\ &(\text{total allowed resources}) = (\text{allowed resources}) \\ &\quad \cup (\text{resources in an allowed role}) \\ &\quad \cup (\text{included-in-function resources in an allowed role}) \\ &\quad \cup (\text{included-in-allowed-function resources}) \\ &(\text{total rejected resources}) = (\text{rejected resources}) \\ &\quad \cup (\text{resources in a rejected role}) \\ &\quad \cup (\text{included-in-function resources in a rejected role}) \\ &\quad \cup (\text{included-in-rejected-function resources}) \end{aligned}$

According to a change in the authority information, a resource into which an identity is generated and a resource from an identity is deleted are determined. For

example, when it is assumed that a user uses systems S1 and S2 from among systems S1, S2, and S3 according to an existing authority, and it is calculated that the authority of the user is changed to use the systems S2 and S3, an identity deletion operation is performed on the system S1, an identity generation operation is performed on the system S3, and only when the authority to the system S2 is changed, is an identity changing operation performed on the system S2 that is continuously used.

The resource-associated user calculation algorithm is illustrated by a flowchart of FIG. 6. Referring to FIG. 6, to-be-changed-authority resource associated user information is inquired about and set to a set A (operation 501), authorities of an organization and a user is changed (operation 503), and to-be-changed-authority resource associated user information is inquired about and set to a set B (operation 505). Resource-associated user provision information may be configured as illustrated in FIG. 6. Specifically, in operations 501 and 505, the resource-associated user provision information can be configured as a Hashtable including a to-be-processed (added/amended/deleted) user information list by using a resource as a key. In the two aforementioned operations, a to-be-changed-authority refers to organizations or users that grant an authority. Next, identities of users who are included in the set A-B are deleted and the identities are added to a list (operation 507), identities of users who are included in the set B-A are added and the identities are added to a list, and users who are included in the set $A \cap B$ are calculated (operation 511)..

Next, individual user information is inquired about (operation 513) to determine whether or not user-associated operation calculation is completed (operation 515). When the operation calculation is not completed, a user-included set is determined (operation 517). When the user-included set is the set B-A (operation 520), the set $A \cap B$ (operation 530), or the set A-B (operation 540), resource identity creation and list addition (operation 521), resource identity update and list addition (operation 522), or resource identity deletion and list addition (operation 525), is performed, respectively.

The resource authority component 240 obtains authority information regarding users in the resource 300 according to a resource authority calculation method, and transmits user identity and authority (role/function) information to the resource adaptor 270. The resource authority calculation method is performed as follows.

$$\begin{aligned}
 &(\text{resource role}) = (\text{total allowed roles in allowed resources}) - (\text{total rejected roles in allowed resources}) \\
 &(\text{function}) = (\text{total allowed functions in allowed resources}) - (\text{total rejected functions in allowed resources}) \\
 &(\text{total allowed functions}) = (\text{allowed functions}) \cup (\text{functions in allowed roles}) \\
 &(\text{total rejected functions}) = (\text{rejected functions}) \cup (\text{functions in rejected roles})
 \end{aligned}$$

The resource adaptor 270 performs generation, change, deletion, and authority synchronization of identities on an associated system by using the identity management operation for the resource 300 obtained by the provisioning component 210 and identity and authority information regarding resources obtained by the resource authority component 240.

The resource provisioning method according to the identity management operations will now be described. Management operations for groups and users occur as described in the following table according to resources in consideration of authority inheritance.

operation	resource adaptor operation
user addition	identity addition and authority synchronization
user authority change	identity/authority deletion for a resource without a usage authority authority synchronization when an authority for an existing used resource is changed identity addition and authority synchronization for all resources that are being used.
user deletion	identity/authority deletion from all resources that are being used

user group migration	since an inherited authority can be changed, user authority change and the same operation occurrence
group addition	group generation in a resource
group authority change	
group migration	since an inherited authority can be changed, group authority change and the same operation occurrence
group deletion	group deletion from a resource
role member change	<p>for all users influenced by groups, an operation of changing authorities of users according to resources is calculated to call a resource adaptor only once according to resources.</p> <p>the resource adaptor performs the user authority changing operation on all users to be changed.</p>
role deletion	since a usage authority for role members (resource, function) is deleted, changes in user authorities (identity addition/deletion, etc) such as changes in role members for all users who have an inheritance and use roles occur
function deletion	since a usage authority for a function is deleted, changes in user authorities (identity addition/deletion, etc) for all users who have an inheritance and use functions occur

A data model in a resource provisioning process according to an embodiment of the present invention will now be described.

FIG. 7 illustrates initial data used for resource provisioning according to an embodiment of the present invention. First, a premise configuration is described as

follows.

The general affairs team is subordinate to the general affairs department.

Hong Gil-Dong is a user included in the general affairs team.

A KM user uses a KM resource, and the KM resource has a knowledge inquiry function.

A GW user uses a GW resource, and the GW resource has a mail transfer and payment function.

The general affairs department inherits a KM user role.

-> Hong Gil-Dong uses the KM resource and has the knowledge inquiry function.

Consequently, Hong Gil-Dong has an identity and an authority over the KM resource.

FIG. 8 illustrates a data model after a function allowance operation is performed.

- 5 In the embodiment, after a GW manager role is allowed for Hong Gil-Dong, Hong Gil-Dong has the GW user authority. The provisioning operation performed by using the data model illustrated in FIG. 8 is described as follows.

The provisioning component calculates that Hong Gil-Dong uses the GW resource, and Hong Gil-Dong uses the KM resource.

- Since the KM resource has been used, an operation of updating an authority is obtained for the KM resource as needed.
- Since the GW resource is newly allocated, an operation of generating a Hong Gil-Dong identity is obtained for the GW resource.

The resource authority component

- obtains a knowledge inquiry authority of Hong Gil-Dong for the KM resource.
- obtains the mail transfer, payment authority of Hong Gil-Dong for the GW resource.

The resource adaptor

- generates an identity of Hong Gil-Dong for the GW resource and registers the mail transfer, and payment authority.

Finally, Hong Gil-Dong has the identity and authority over the KM resource and GW resource.

FIG. 9 illustrates a data model after a function rejecting operation is performed.

First, when the knowledge inquiry function for Hong Gil-Dong is rejected, although Hong Gil-Dong has the knowledge inquiry authority due to the KM user authority, since the knowledge inquiry authority is additionally set to be rejected, Hong Gil-Dong does not have the knowledge inquiry authority finally. The knowledge inquiry authority is an authority of the KM resource. However, since Hong Gil-Dong does not have any authority of the KM resource currently, Hong Gil-Dong does not have an identity of the KM resource.

The provisioning operation performed by using the data model illustrated in FIG. 9 is described as follows.

<p>The provisioning component calculates that Hong Gil-Dong is using the GW resource.</p> <ul style="list-style-type: none"> - Since the KM resource is not used, an operation of deleting an identity of Hong Gil-Dong from the KM resource is obtained. - Since the GW resource has been used, an operation of updating an authority over the GW resource is obtained as needed.
<p>The resource authority component obtains the mail transfer and payment authority of Hong Gil-Dong for the GW resource.</p>
<p>The resource adaptor deletes the identity of Hong Gil-Dong from the KM resource.</p>

Consequently, Hong Gil-Dong has the identity and authority over the GW resource.

The invention can also be embodied as computer readable codes on a computer readable recording medium. The computer readable recording medium is any data storage device that can store data which can be thereafter read by a computer system. Examples of the computer readable recording medium include read-only memory (ROM), random-access memory (RAM), CD-ROMs, magnetic tapes, floppy disks, optical data storage devices, and carrier waves (such as data transmission through the Internet). The computer readable recording medium can also be distributed over

network coupled computer systems so that the computer readable code is stored and executed in a distributed fashion.

INDUSTRIAL APPLICABILITY

5 In an integrated identity management market, customers want to manage an authority of an associated resource as well as an identity. Using the method according to the embodiment of the present invention, customers can have the following advantages.

10 1) A function and a role in a resource can be defined. 2) A role including a resource can be defined as a shared role. 3) An authority (role, resource, function) can be allocated as allowance or rejection to an organization and a user. Accordingly, an authority allocated to a final user can be easily inquired about. 4) The provisioning system can provision an identity according to resources allocated to a final user and provision an authority (function and role) in resources, so that integrated identity and
15 authority management can be implemented in the center.

CLAIMS

1. An authority-based resource identity and authority provisioning apparatus for integrated identity management, comprising:

a management application which performs organization/user authority setting;

5 a provisioning component which operates resource-associated users by using authority information set by the management application to generate resource-associated user provision information;

10 a resource authority component which performs parallel processing on the generated resource-associated user provision information according to resources to calculate an authority in a resource according to users; and

a resource adaptor which performs an identity operation by using information on the calculated authority in a resource according to users,

wherein the identity operation includes user identity generation, identity change, and identity deletion, and

15 wherein all user identity operations are performed according to resources.

2. The apparatus of claim 1, wherein the authority information set by the management application includes "authority allowance" for users, and "authority allowance inheritance" and "authority rejection inheritance" for organizations.

3. The apparatus of claim 1, wherein the management application includes an authority setting user interface which includes authority types (role, resource, and menu), a selected authority display, and a resource selection window.

25 4. The apparatus of claim 1, wherein the provisioning component uses role/resource/function information data in order to generate resource-associated user provision information by operating resource-associated users.

30 5. The apparatus of claim 1, wherein the provisioning component has a function of converting an "organization/user/authority management operation" into a "resource-associated identity and authority provisioning operation", obtains information regarding an associated resource to be provisioned to a user from the authority information, and transmits resource-associated operation information to the resource

authority component.

6. The apparatus of claim 1, wherein a resource calculation method used by the provisioning component is as follows.

5

$\begin{aligned} \text{(to-be-provisioned resources)} &= \text{(total allowed resources)} - \text{(total rejected resources)} \\ \text{(total allowed resources)} &= \text{(allowed resources)} \\ &\cup \text{(resources in an allowed role)} \\ &\cup \text{(included-in-function resources in an allowed role)} \\ &\cup \text{(included-in-allowed-function resources)} \\ \text{(total rejected resources)} &= \text{(rejected resources)} \\ &\cup \text{(resources in a rejected role)} \\ &\cup \text{(included-in-function resources in a rejected role)} \\ &\cup \text{(included-in-rejected-function resources)} \end{aligned}$

7. The apparatus of claim 1, wherein the resource-associated user calculation is performed by using:

10 a unit which inquires about to-be-changed-authority resource associated user information and setting the information to a set A;

a unit which changes an authority of an organization and a user;

a unit which inquires about to-be-changed-authority resource associated user information and setting the information to a set B;

15 a unit which deletes identities of users who are included in the set A-B and adding the identities to a list, deleting identities of users who are included in the set B-A and adding the identities to a list, and calculating users who are included in the set $A \cap B$;

a unit which determines whether or not a user-associated operation calculation is completed by inquiring about individual user information; and

20 a unit which determines a user-included set when the operation calculation is not completed, and performing resource identity creation and list addition, resource identity update and list addition, or resource identity deletion or list addition when the

user-included set is the set $B-A$, the set $A \cap B$, or the set $A-B$, respectively.

8. The apparatus of claim 7, wherein the resource-associated user information is configured as a Hashtable including a to-be-processed
5 (added/amended/deleted) user information list by using a resource as a key.

9. The apparatus of claim 1,
wherein the resource authority component obtains authority information regarding users in the resource according to a predetermined resource authority
10 calculation method, and transmits user identity and authority (role/function) information to the resource adaptor, and

wherein the resource authority calculation method is performed as follows.

(resource role) = (total allowed roles in allowed resources) - (total rejected roles in allowed resources)

(function) = (total allowed functions in allowed resources) - (total rejected functions in allowed resources)

(total allowed functions) = (allowed functions) \cup (functions in allowed roles)

(total rejected functions) = (rejected functions) \cup (functions in rejected roles)

15 10. The apparatus of claim 1, wherein the resource adaptor performs generation, change, deletion, and authority synchronization of identities on an associated system by using the identity management operation for the resource obtained by the provisioning component and identity and authority information regarding resources obtained by the resource authority component.

20

11. A computer-readable medium having embodied thereon a computer program for implementing the apparatus of any one of claims 1 to 10.

FIG. 1

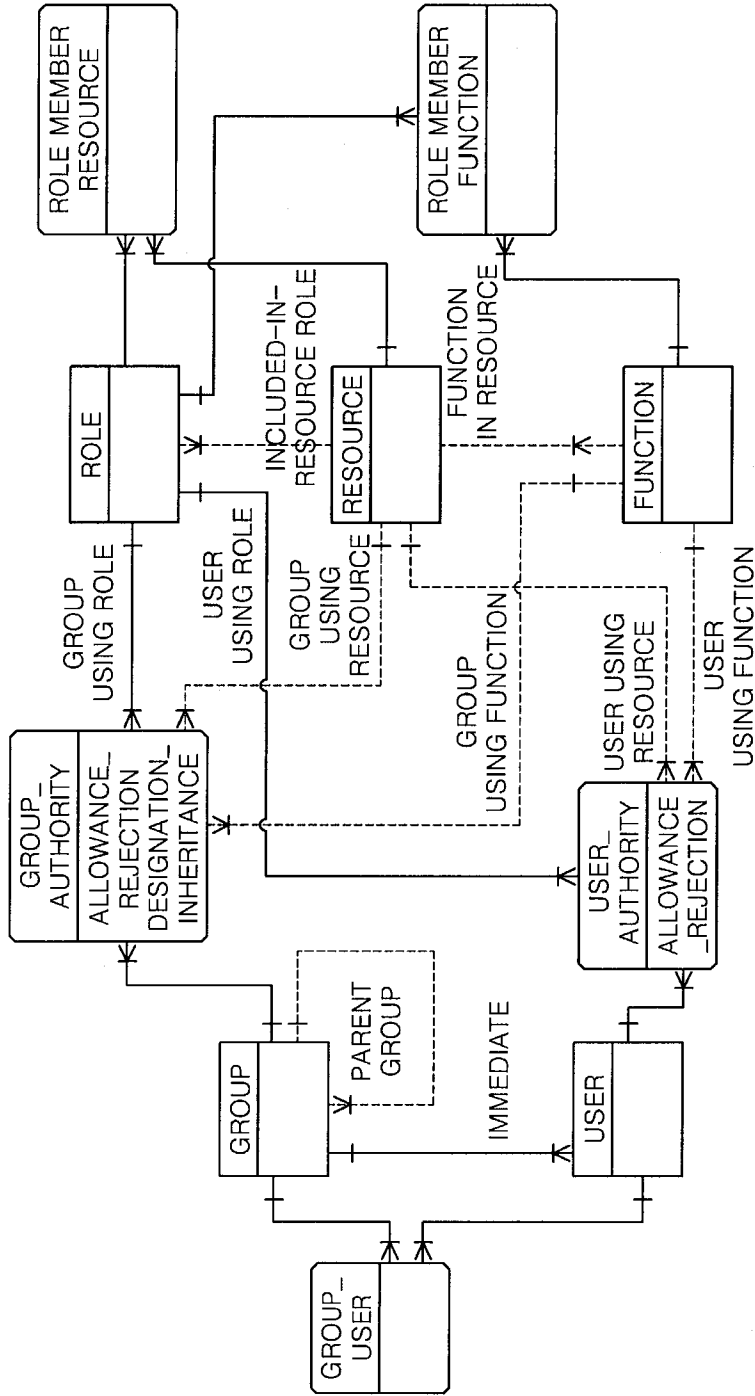


FIG. 2

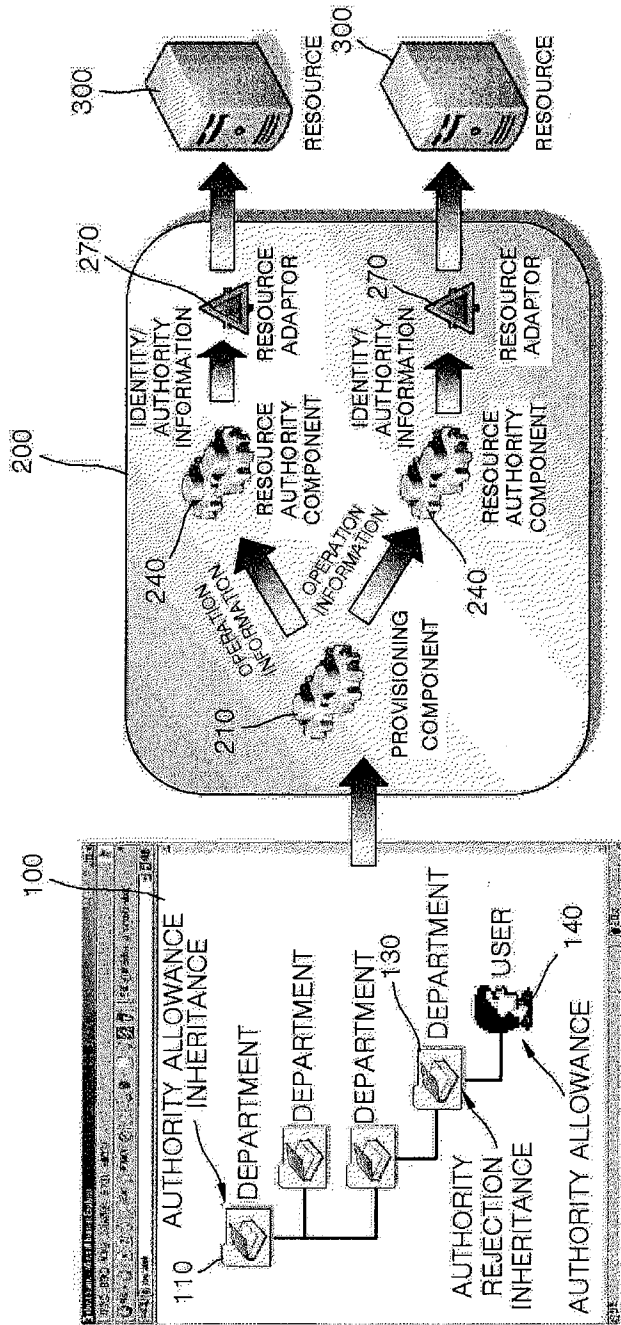


FIG. 3

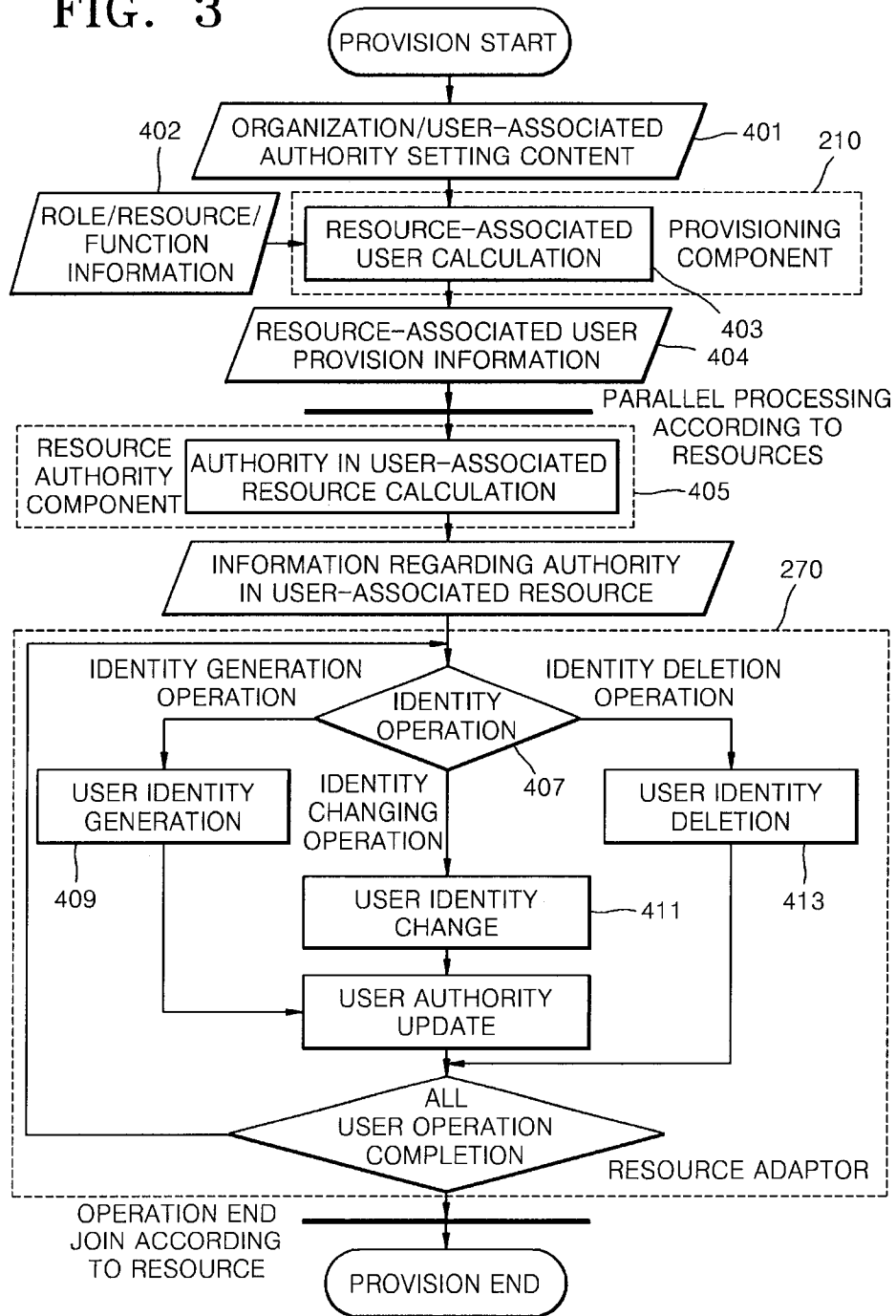


FIG. 4

AUTHORITY TYPE { ROLE RESOURCE MENU }
 SELECTED ITEM: ROLE RESOURCE START END RANKING
 ALLOWANCE INHERITANCE USER (PUBLIC) CURRENT PERMANENT 5
 SELECTED AUTHORITY

RESOURCE SELECTION
 ITEM TO BE SELECTED
 [TOTAL] RESOURCE
 PERSONAL AND BASIC INFORMATION MANAGER DemoERP
 PERSONAL INFORMATION MANAGER DemoERP
 ATTENDANCE MANAGER DemoERP
 ATTENDANCE AND WAGE MANAGER DemoERP
 WAGE MANAGER DemoERP
 BASIC DATA MANAGER DemoERP
 TOTAL MANAGER DemoERP
 INQUIRY AND OUTPUT MANAGER DemoERP
 MIS_ROLE DemoERP

ADD DELETE
 START DATE CURRENT DEFINED
 END DATE PERMANENT DEFINED
 AUTHORITY ALLOWANCE 5-NORMAL

FIG. 5

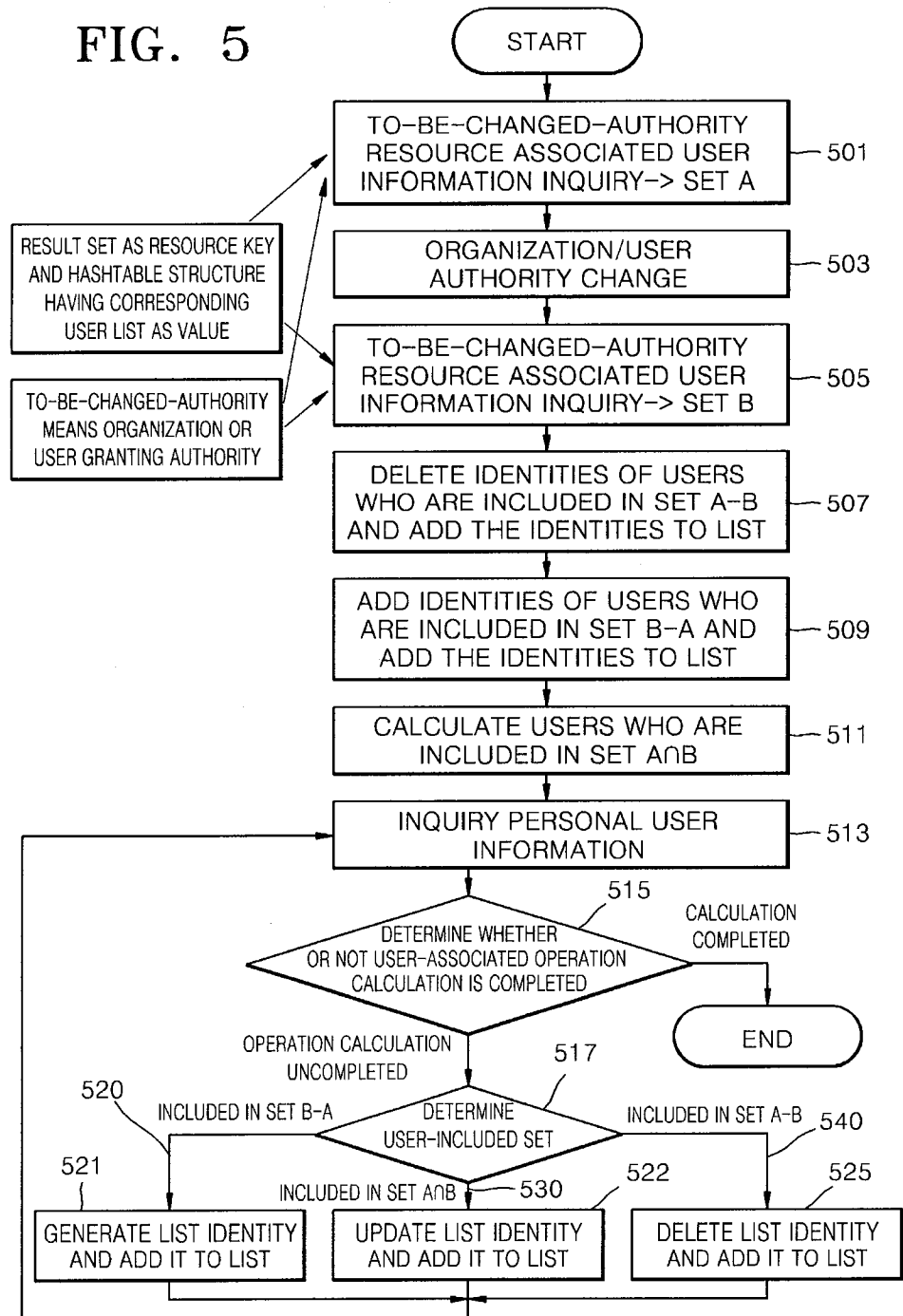


FIG. 6

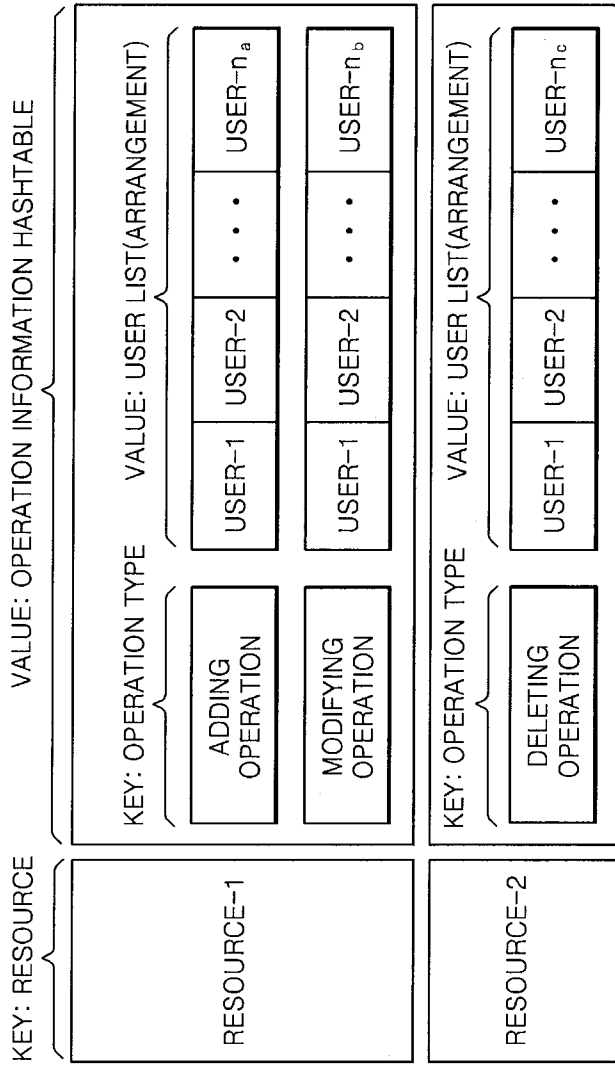
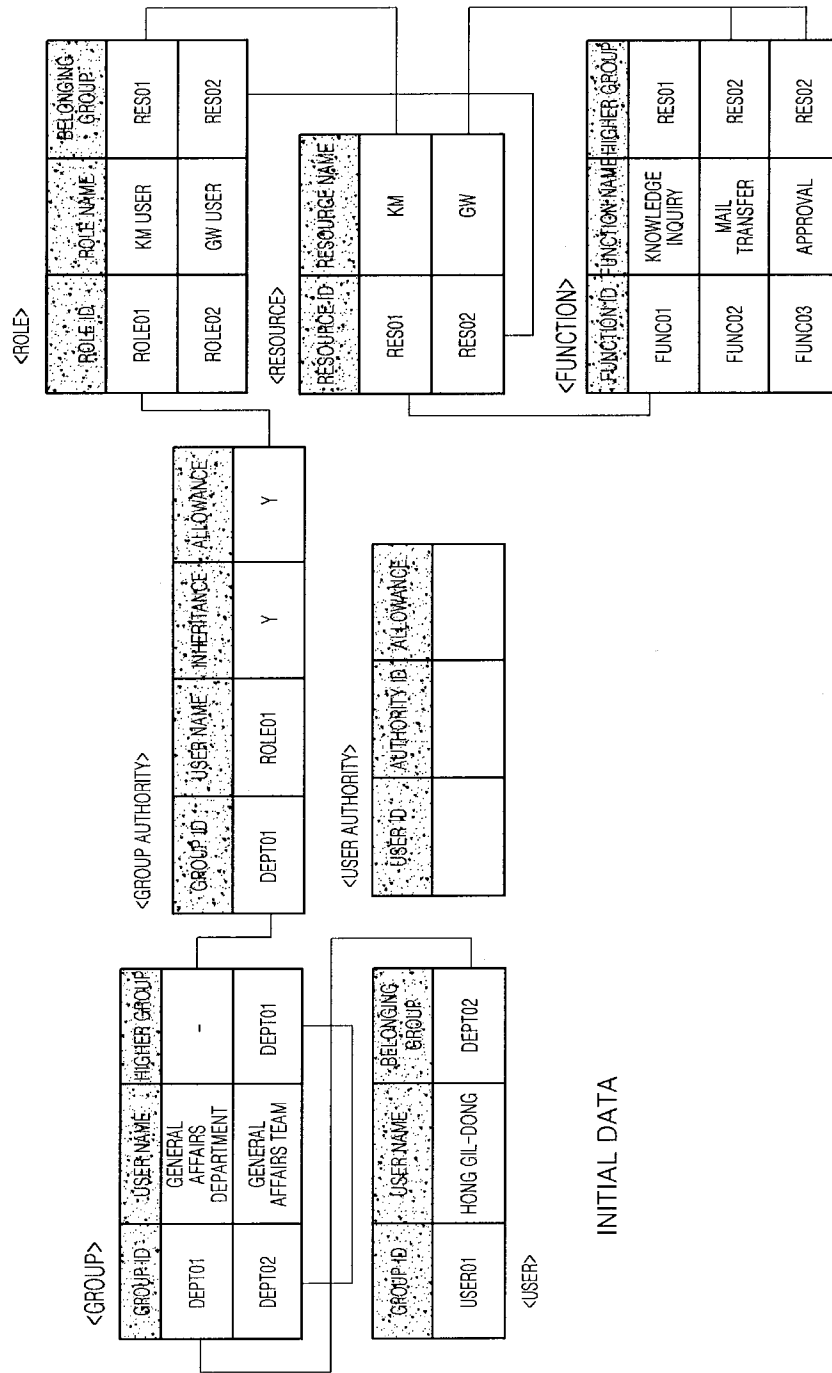
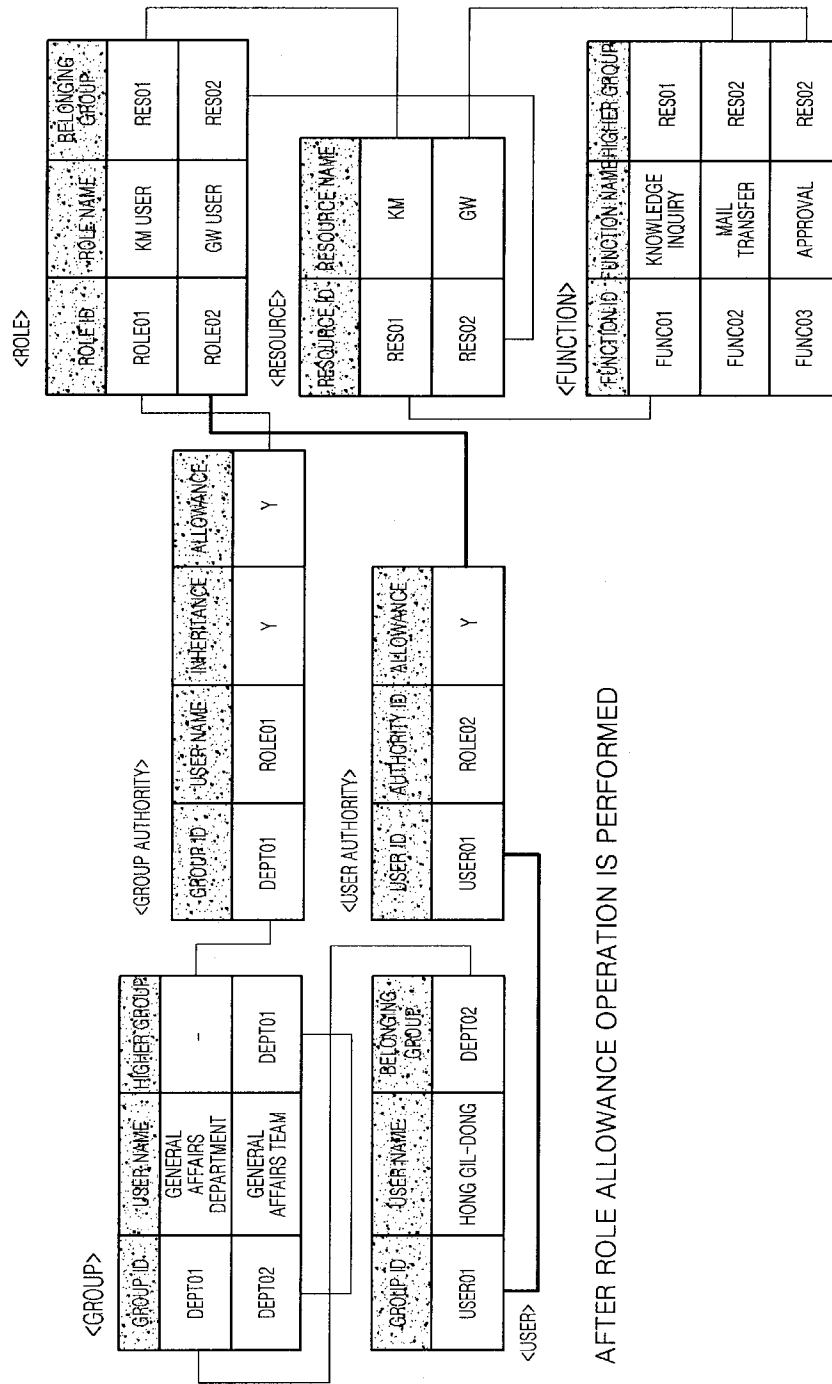


FIG. 7



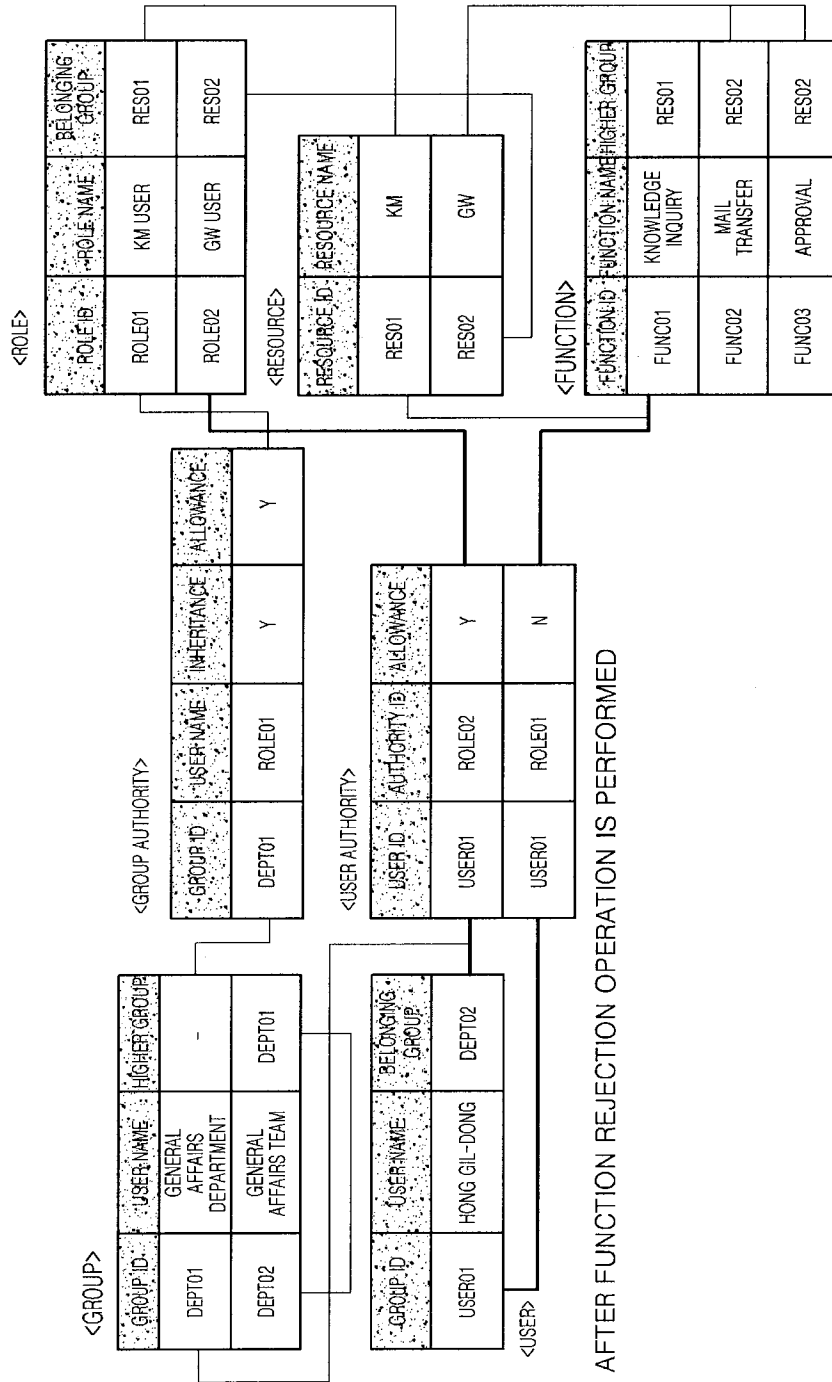
INITIAL DATA

FIG. 8





AFTER ROLE ALLOWANCE OPERATION IS PERFORMED

FIG. 9



INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2007/003594

A. CLASSIFICATION OF SUBJECT MATTER		
<i>G06F 15/00(2006.01)i</i>		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) IPC 8 : G06F 11/30, G06F 17/30		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Korean Utility Models and applications for Utility Model since 1975 Japanese Utility Models and applications for Utility Model since 1975		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) eKIPASS(KIPO internal) "identification", "right", "role"		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2002/0026592 A1 (GAVRILA SERBAN I. et al.) 28 February 2002 See abstract, Figure 3, paragraphs [0019]-[0044], claims	1, 11 --- 3
Y	US 2005/0240996 A1 (HITCHCOCK DANIEL WADE) 27 October 2005 See abstract, Figure 3, paragraphs [0020] -[0037], claims	3
A	US 6950825 B2 (CHANG DAVID YU et al.) 27 September 2005 See abstract, claims	1-11
A	US 6757680 B1 (CHOY DAVID MUN-HIEN) 29 June 2004 See abstract, claims	1-11
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 11 MARCH 2008 (11.03.2008)		Date of mailing of the international search report 11 MARCH 2008 (11.03.2008)
Name and mailing address of the ISA/KR  Korean Intellectual Property Office Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140		Authorized officer LEE, Jong Iek Telephone No. 82-42-481-8373 

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2007/003594

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002/0026592 A1	28.02.2002	NONE	
US 2005/0240996 A1	27.10.2005	AU 2005201002 A1 BR 200500970 A CA 2500618 AA CN 1691573 A EP 01589398 A2 JP 2005310125 A2 KR 1020060043725 A RU 2005108108 A	10.11.2005 06.12.2005 23.10.2005 02.11.2005 26.10.2005 04.11.2005 15.05.2006 10.10.2006
US 6950825 B2	27.09.2005	US 20030229623 A1	11.12.2003
US 6757680 B1	29.06.2004	NONE	