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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 September 2012 (27.09.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/126528 A1

(51) International Patent Classification:
G06F 21/24 (2006.01) *H04L 29/06* (2006.01)

(21) International Application Number:
PCT/EP2011/054538

(22) International Filing Date:
24 March 2011 (24.03.2011)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **ATOS IT SOLUTIONS AND SERVICES GMBH** [DE/DE]; Otto-Hahn-Ring 6, 81739 München (DE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **GEHRTZ, Udo** [DE/DE]; Saalestraße 44, 51371 Leverkusen (DE). **ORZESSEK, Dieter** [DE/DE]; Dechant-Wessing-Str. 37, 45663 Recklinghausen (DE).

(74) Agent: **WILHELM & BECK**; Prinzenstr. 13, 80639 Munich (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, 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, KR, 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, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

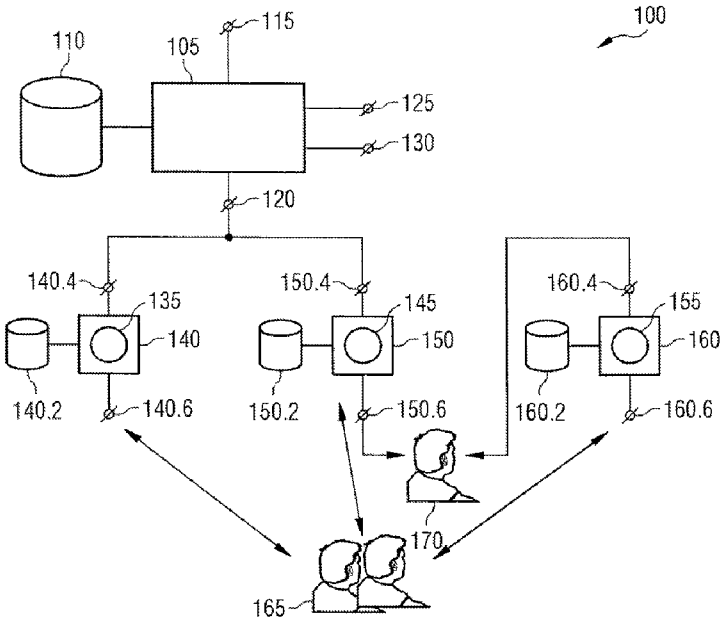
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: SYSTEM AND METHOD FOR USER ACCESS MANAGEMENT

FIG 1



(57) Abstract: System and method for user access management The invention relates to a system for managing permissions of a user to a plurality of services, wherein the services have separate permissions databases and each permissions database holds a portion of the user's permission information. The system comprises a first interface for accepting a first request for accessing permissions of the user to the services, a repository with information indicative of a first association between the user and at least one user group and a second association between the at least one user group and access permissions to at least one of the services. The system further comprises a processing unit for determining, on the basis of the information in the repository, permissions to be set in the permissions databases of the at least one service and a second interface for sending second requests to administration interfaces of the at least one determined service to effect access to the determined permissions. The invention further relates to a corresponding computer program product and a corresponding method for managing access permissions of the user.

WO 2012/126528 A1

Description

System and method for user access management

State of the art

An institution like a company or school may run a number of networked computers on which services such as e-mail, directory, database and others are offered. Generally, use of the services is restricted to a limited number of users so that user permissions must be kept and service access policies must be enforced. It is common that at least some of the services make use of local permissions databases in which information on users and their access privileges are kept. In this case it may be necessary to synchronize some of the information between the different databases.

Synchronization is often made more difficult by other factors. For instance, the number of offered services tends to increase over time, gradually raising complexity of the synchronization task. In some cases, a service may be moved to a third party hoster, where it is more difficult to access the permissions information. In another case, a service may be split up into several sub-services or several services may be joined into one, for instance when the institution running the services is expanded or split, which means that permissions information must be split or joined accordingly.

Furthermore, some of the systems may have to be accessed from users or institutions outside of the company. This may apply to mobile workers but also to other institutions who share business processes with the first institution on a business-to-business (B2B) integration basis. In this case, the services may be accessible through a portal and different types of integrated businesses may be associated with predetermined permissions on a predetermined set of the services. In case the status of an integrated institution changes, for instance because an existing collaboration is

intensified or terminated, the permissions of the respective users of the integrated institution must be updated accordingly. They may require the orchestrated change of many bits of information in a number of different permissions databases of the different services in different places and under control of different organizational sections of the institution.

It is an object of the invention to provide a system and a method for facilitating user permissions management in the described scenario. The invention achieves the given object through a system with the features of claim 1 and a method according to the features of claim 12. Dependent claims specify preferred embodiments.

Disclosure of the invention

According to the invention, a a system for managing permissions of a user to a plurality of services, wherein the services have separate permissions databases and each permissions database holds a portion of the user's permission information is provided. The system comprises a first interface for accepting a first request for accessing permissions of the user to the services, a repository with information indicative of a first association between the user and at least one user group and a second association between the at least one user group and access permissions to at least one of the services. The system further comprises a processing unit for determining, on the basis of the information in the repository, permissions to be set in the permissions databases of the at least one service and a second interface for sending second requests to administration interfaces of the at least one determined service to effect access to the determined permissions.

According to the described system, it may no longer be required to support a synchronization mechanism for permissions information between the various permissions

databases of the services. Instead, all relevant changes may be initiated from a central point of access which can be used to manage user permissions even in a complex infrastructure of a large number of services of different types, in different places, under control of different sub-organizations and with arbitratry dependencies.

The global permissions database may provide an additional source of information with can be used to find out which of the services hold what specific information on a predetermined user. Also, by using a role based permissions system it can be made sure that every user has permissions that reflect his functionality with respect to the service structure. Using this, administration of user accounts may be entrusted to a contractor without the risk of unauthorized change of privileges to a user account. This may help making a complex server installation with frequent changes to user accounts practically manageable.

The system may also comprise a global permissions database for storing the determined permissions of the user. The global permissions database may serve as a repository for an overview of user permissions. Statistical and billing information may be drawn from the global permissions database. The global permissions database may also be used for legal purposes in that it may be proved what access privileges were modified through the system and under what circumstances.

The system may also comprise a third interface for accepting a response from at least one of the services about whether or not said second request to the service has been carried out, wherein the system is adapted to update the user's permissions in the global permissions database according to the response.

The global permissions database may thus give a matching picture of what has actually been done to the services'

permissions databases. This may be advantageously used to increase a level of coherence between the different permissions databases. In case of problems in user access management, like a failed creation of a user account with one of the services, the global permissions database may serve as a reference. By finding out which permissions database of which service does not comply with the global permissions database, problems in user permissions may be pinpointed.

In a preferred embodiment, the global permissions database does not store a specific value of a user permission, but the existence of the corresponding attribute instead. For instance, the information that a user has access permission of a certain group on a certain service may be kept in the global permissions database but the user's actual credentials may neither be kept in the global permissions database nor synchronized with the service's database. This way, service access especially for users from B2B-integrated external institutions may be replicably managed through said system with said global permissions database.

In another preferred embodiment, the effected access to the user's permissions in the service's permissions databases comprises write-only accesses. For instance, the access may be restricted to creating, amending and deleting permissions of the user from the permissions databases of the affected services. Not reading the permissions from the backend services may help avoiding a large collection of sensitive information that may be subject to unauthorized access. It may also help designing an easy to implement infrastructure with the services as a secure retrieving of sensitive information is not required.

The system may further be adapted to return, upon a corresponding request, information indicative of a plurality of users who possess a predetermined access permission. This information may be used to assess various security related characteristics of the services.

For instance, the global permissions database may be queried to return information on software licenses that are due according to the existing user accounts. This may help keeping license expenses low. In another example, the global permissions database may be consulted for existing accounts when a user account is to be globally deleted, thus helping to make sure no stray user account is left on one of the services. License cost may therefore be further lowered and service security may be increased.

The system may also be adapted to return, upon a corresponding request, information indicative of a history of accesses to a user's permissions. This feature may profitably be used in an audit trail. Collecting and consolidating access logs from the various services may therefore be made obsolete. This way, compliance with legal regulations may be enforced and security on the services may be further enhanced.

In one embodiment, the administration interface of one of the services may comprise an electronic mailbox (email). The information in the mailbox may be parsed and processed automatically, e.g. as part of the service, or a human administrator may read the request in the mailbox and act appropriately. Electronic mail is often easily available and a human administrator may provide a flexible and adaptable connection between the request and the actual access to the permissions database of the service. Messages sent to the corresponding email address may also be forwarded to a trouble ticket system.

In another embodiment, one of the administration interfaces of the services may comprise a machine interface for direct access to the user's permissions on the database of the service. The machine interface may e.g. use messages according to the SOAP, CORBA or any other standard for information interchange.

The system may be adapted to reject the first request in case predefined data associated with the first request is not available to the system.

In this way, access to any of the services may be held back until sufficient information is present for access to all of a predetermined set of services. This may help to prevent partial execution of the first request which might otherwise lead to an unclear or even contradictive status of user permissions in the permissions databases of the services. It may also help enforcing an approval process for the request.

Preferably, the global permissions database is adapted to be located on a server that is different from a server on which the interfaces and the processing unit reside. In this way, the database may be kept in a separated environment which may offer additional safety features, such as interface communication filtering, firewalling, regular backup, disaster recovery and other related measures.

In one embodiment, the global permissions database resides on a virtual server which is hosted on a plurality of physical servers. This may help to keep an availability of the general permissions database high even in the case of failure of one of the physical servers.

According to another aspect of the invention, a method for managing access permissions of a user to a plurality of services, the services having separate permissions databases, each permissions database holding a portion of the user's permission information, comprises steps of: receiving a first request for accessing permissions of the user, determining permissions to be set in the permissions databases of the at least one service on the basis of information indicative of a first association between the user and at least one user group and a second association between the at least one user group and access permissions to at least one of the services

and sending second requests to administration interfaces of the at least one determined service to effect access to the determined permissions.

The method may advantageously be carried out on the above-mentioned system, which may comprise a computer system.

According to a third aspect of the invention, a computer program product for carrying out said method may be executed on a processing device or stored on a computer-readable medium.

Brief description of the Figures

The invention will now be exemplified with reference to the enclosed Figures, in which:

Figure 1 shows a system for user access management;

Figure 2 shows a repository 200 for a group based permission scheme.

Figure 3 shows another embodiment of the system of Figure 1;

Figure 4 shows a schematic diagram of a method for user access management;

Figure 5 shows a schematic diagram of a method for retrieving an audit trail; and

Figure 6 shows a schematic diagram of a method for computing a number of licenses in use.

Detailed description of embodiments

Figure 1 shows a system 100 for user access management. The system 100 comprises processing a unit 105 which is connected

to a global permissions database 110. The processing unit 105 is also connected to a first interface 115, a second interface 120, a third interface 125 and a fourth interface 130. The interfaces 115 to 130 may be adapted to conduct information that relates to a human input or output or they may be adapted to conduct machine information such as an electronic representation of an object, a message or a signal. In further embodiments of the system 100, some or all of the interfaces 115 to 130 may be combined into one interface.

A first service 135 is implemented on a first backend server 140 which comprises a first permissions database 140.2, a first administration interface 140.4 and a first service interface 140.6. Similarly, second and third services 145 and 155 are implemented on second and third backend servers 150 and 160, respectively.

One or more users 165 may communicate with the servers 140, 150 and 160 through the associated service interfaces 140.6, 150.6 and 160.6 to obtain access to the services 135, 145 and 155, which may e.g. comprise services of e-mail, database, access, purchase, organization and management services. The servers 140, 150 and 160 are called backend servers because to users 165 who stand outside of an organization that runs the system 100 and/or the services 135, 145 and 155, access to the servers 140, 150 and 160 is performed from external, usually through a security component such as a packet filtering firewall or a portal.

Administration interfaces 140.4 and 150.4 of first and second backend servers 140, 150 are each connected to the second interface 120 of the system 100. In order to manage permissions of a user 165 to the services 135 and 145, particularly for creating or deleting the user 165 in the permissions databases 140.2 and 150.2, a corresponding request is sent to the first interface 115 of system 100. After passing optional tests pertaining to the presence of

required data, e.g. user name and user group, the system 100 sends out messages through the second interface 120 to effect the requested change of information in the permissions databases 140.2 and 150.2. Preferably, a confirmation is sent back to the system 100 from the services 135, 145 so that it is known in the system 100 that the requested access has been carried out. Information on what user permissions have been created, modified or deleted for services 135, 145 on corresponding permissions databases 140.2, 150.2 is then written to the global permissions database 110.

In Figure 1, the system 100 is able to effect the user permissions access directly through a machine-to-machine communication through the second interface 120 and the administration interfaces 140.4, 150.4 of backend servers 140, 150, respectively. Where this is not possible, e.g. for the third service 155 on the third backend server 160, the access to user permissions in the database 160.2, which is associated to third service 155, may be carried out through a human administrator 170.

In the example of Figure 1, service 145 is an e-mail or a similar groupware or message delivery service. Through the second interface 120, an e-mail or corresponding other human-readable message is passed to the second service 145 for delivery to the human administrator 170. To this end, the service interface 150.6 may be used instead of the administration interface 150.4. After the administrator 170 has received the message, he effects the requested user permissions change through the administration interface 160.4 in the third permissions database 160.2. A confirmation that the requested change has been carried out or a notification that at least some of the changes could not be carried out may be sent back by the administrator 170 to the system 100 through the e-mail service 145. In a different embodiment, the notification may be automatically generated and sent from the service 145 to the system 100.

In many cases, it is not necessary that the permissions of the user 165 correlate between permissions databases 140.2, 150.2 and 160.2. The object for system 100 is rather to create and delete accounts for the user 165 in an orchestrated manner for the services 135, 145 and 155. This is particularly true for said external users 165 such as a supplier or a cooperating company.

In order to enable integrated cooperation with a user 165 of an external institution, a user account is created for said user 165 in each of the services 135, 145 and 155. The creation and furnishing with certain access rights is initiated through the system 100 and effected in the appropriate permissions databases 140.2, 150.2 and 160.2. If, at a later point in time, the cooperation with the user 165 is terminated, the user accounts in the permissions databases 140.2, 150.2 and 160.2 for services 135, 145 and 155, respectively, are deleted by initiation through system 100. To this end, the global database 110 is queried for which of the services 135, 145 and 155 an account for the user 165 exists and then corresponding deletion requests are sent out to administration interfaces 140.4, 150.4 and 160.4 of servers 140, 150 and 160, respectively.

Between creating and deleting the user 165 for the services 135, 145 and 155, the global permissions database 110 may be queried through third and fourth interfaces 125, 130 for management purposes. For instance, it may be interesting to see on which of the services 135, 145 and 155 a user 165 has access permissions. This may be done in order to obtain an accounting for user licenses that have to be paid for each of the services 135, 145 and 155.

A corresponding query may be done on a per-service basis. For instance, the number of users 165 who have an account on a predetermined one of the services 135 through 155 may be queried through one of the interfaces 125, 130 of system 100.

Also, a history of changes to user permissions, either on a per-user basis or a per-service basis, may be queried from the global permissions database 110 from the system 100 using one of the interfaces 125, 130.

Figure 2 shows an exemplary repository 200 that is organized in a first matrix 205 and a second matrix 210. Through the matrices 205 and 210 an access permissions management may be enforced that is compatible with system 100 of Figure 1.

The first matrix 205 shows how users 165 are associated to user groups 215. In a vertical direction the users 165 are shown and in a horizontal direction user groups 215 are shown. A user 165 is associated to a group 215 where a mark is shown in the cell that is defined by the user 165 and the user group 215.

The second matrix 210 shows how services are associated to user groups 215. The second matrix 210 holds columns for a ticket tool service 230, electronic mail (email) 235 and a telephone service 240. The systems associated to columns 230-240 correspond to systems 135, 145 and 155 in Figure 1.

Lines of the second matrix 210 are grouped to functionalities "mail" 245, "mobility" 250 and "security" 255. A functionality is comparable to a role or a task and serves to organize the function a user 165 acts in. The functionalities may be permeable, allowing a user 165 to be moved or associated to between different functionalities or users may be restricted to one predetermined functionality.

Cells of the second matrix 210 hold the names of those user groups 215 that are associated with access permissions to the corresponding service. For instance, the "mail" functionality 245 comprises all tasks that may be carried out in order to ascertain proper functioning of the mail system 235. User groups 215 with access permissions to the mail system 235 comprise group "postmaster" 220 and "mail_support" 225. Users

165 who are members of those groups will therefore have permission to access the email system 235 and the ticket tool 230. By defining group access permissions to services by functionalities, it is possible to organize permissions of users 165 to the services 230-240 according to a business perspective.

In an illustrative example, a user 165 may be assigned the "mail" functionality 245. User 165 is therefore assigned to user groups "postmaster" and "mail support", enabling him to use the ticket tool 230 and the email system 235. At this point, there is no way for said user 165 to gain access to the telephone system 240. Permissions as defined in the second matrix 210 are given such that user 165 is enabled to perform the "mail" functionality 245 he is assigned to but his permissions will not reach to systems the user 165 does not need for his functionality.

Should our user 165 later be assigned to the "mobile" functionality 250, he will be made member of other user groups 215 that are specific to the new functionality. In the process, he may lose his membership to the roles 215 that are specific to the "mail" functionality 250. The groups the user 165 must be removed from can be determined by looking up in the second matrix 210 the user groups 215 associated with the functionality the user 165 is removed from. The process of a user 165 entering or changing a functionality may be subject to an approval process, as will be explained later with respect to Figure 4.

The access permissions scheme displayed in Figure 2 does not take into account fine granular permissions that may be given to a user 165 or group 315 on the corresponding services 230-240.

Figure 3 shows another embodiment of the system 100 of Figure 1. System 100 is shown in the centre of Figure 3. A number of backend servers 305 to 335 provide services such as identity

and access management, reporting, charging and billing, contract data, incident and problem management, change and configuration management and access management.

Generally speaking, each service is running on a server, where a server may comprise one or more physical computers and possibly additional hardware such as a storage system. For the purpose of illustrating the invention, it is however irrelevant what hardware a given service is running on, so that a differentiation between a service and the corresponding server is not strictly maintained.

For communication with systems that are internal to the computer installation shown in Figure 3, a dedicated interface 340 may be comprised by the system 100. There may also be a dedicated interface 345 for communicating with a backend server 350 that is hosted at a third party, i.e. outside of the company installation, which may imply use of a dedicated network or access through a certain security component like a firewall or a portal.

The third and fourth interfaces 125, 130 of system 100 may be used to communicate with operational servers 355 and 360, which may provide, e.g. access right documentation and provisioning of access rights.

The first interface 115 of the system 100 is used to communicate with a customer portal 365 which may also serve as central access point for external users 165. The customer portal 365 may provide a web-based interface and the user 165 may use this interface to place a request to access his/her permissions on the various backend servers 305 to 335 and 350 to the first interface 115. The same first interface 115 may also be used from inside of the installation. While some such requests for access will be handled by the services 305 to 335 and 350, e.g. password change, other requests for access that may touch a security policy or the creation or deletion

of a user account on a service 305 to 335 and 350 may be handled through system 100.

A customer interface 370 provides business-to-business interfaces to permit integration of the services 305 to 335 and 350 over the bounds of said installation. The second interface 120 may be used to communicate with the customer interface 370.

The system 100 may be adapted to support a first process 375 for managing access approval. An access request received through the first interface 115 may be run through the access-approval process before any permission information is touched on any of the backend servers 305 to 335 and 350.

System 100 may also support a second process 380 of documentation and provisioning orchestration. The second process 380 may be used to organize information inside of the global permissions database 110 according to the requirements of access rights documentation 355 and provisioning 360 of access rights. The same process 380 may also control the exchange data via the third and fourth interfaces 125, 130.

Figure 4 shows a schematic diagram of a method 400 for user access management. Method 400 may be executed on system 100 of Figures 1 or 2 or implement the first process 375 of access approval shown in Figure 3.

In a first step 405, a request for accessing a user's permissions is received. The request may comprise a call for user creation, deletion or modification of permissions for one or more services. In one embodiment, the received request implies only the writing of information to one or several permissions databases of services 140, 150, 160, 305 and 335 and 350.

In a following step 410, a check is made if the requested access to user permissions is covered by a group policy. To

this end, one or several groups that the user is in are determined and permissions associated to the groups are retrieved. If the requested access exceeds those permissions, method 400 terminates in a step 415.

In the negative, approval for the requested access is sought in a step 420. This may comprise interaction with a human administrator. Should the approval not be granted, method 400 terminates in step 415. In one variant, the approval step 420 may be omitted or automatic verification and approval may be given.

After approval, in a step 425, the backend servers hosting the requested services are identified. Next, in a step 430, the information and possibly the documents that are required for access to said backend servers are determined. In a step 435, it is reassessed if the documents and/or information are complete. Such information may comprise a user name and address and documents may comprise a picture of the user or a written consent to the intended usage of user specific data.

As long not all required information and documents are present, more information and/or documents are retrieved in a step 440. This may comprise sending back a request for said missing entities to the person or system that initiated method 400 in step 405. When it is found in step 435 that all information and documents required are present, method 400 proceeds with a step 445.

In step 445, messages are sent to the administration interfaces 140.4, 150.4, 160.4 that correspond to the backend servers 140, 150, 160, 305 to 335 and 350 that host the services for which permission information is to be accessed. the sent messages effect the access to said user permissions so that afterwards, user permissions in the permissions databases of the servers 305 to 335 and 350 reflect the desired changes in a concerted fashion.

In an optional step 450, responses from said backend servers are received and evaluated so that it is clear which user permission access has succeeded and which one has failed.

Information that is indicative of the user permissions access is then stored in the global permissions database 110 in a following step 455. This operation may comprise appending an entry to an access history.

It is often necessary for a user 165 to have access to a first service in order to be able to use a second service. For example, using an e-mail service may rely on using a corporate directory. While the request received in step 405 may be simply targeted at enabling e-mail for a specific user 165, the messages sent out in step 445 may comprise several parametrized messages to several services. In the given example, a first message may be sent to the administration interface of the corporate directory server with the request to grant access of said user 165 to a predetermined kind of data, and a second message may be sent to the administration interface of the e-mail server with the request to create a mailbox for the user 165. The mailbox may be created with predetermined parameters for options like a quota or maximum message size and the predetermined parameters may stem from the group policy determined in step 410.

Figure 5 shows a schematic diagram of a method 500 for retrieving an audit trail. Method 500 may be carried out on system 100 of Figures 1 and 2 and may be comprised by the second process 380 of documentation and provisioning orchestration in Figure 3.

In a first step 505, a request for an audit trail is received. Following that, in a step 510, the required information is determined on the basis of a format used in the request and the structure of information inside of the global permissions database 110.

Then, in a step 515, the global database 110 is queried, the information is retrieved and, where necessary, rearranged so as to fit an expected response format for the request received in step 505. In a final step 520, said information is returned and method 500 terminates.

Figure 6 shows a schematic diagram of a method 600 for computing a number of licenses in use. Method 600 is also adapted to be carried out on system 100 of Figures 1 and 2 and may be comprised by second process 380 of documentation and provisioning orchestration of Figure 3. The licenses may be software licenses for a given service, e.g. e-mail.

In a first step 605, a request for a number of licenses is received. The request may be directed at the number of licenses in use for a specific user 165 or a predetermined group of users 165. The request may alternatively be directed at the number of licenses that are in use by a predetermined service 135, 145, 155.

In a following step 610, the required information is determined and requests are generated depending on the way information is organized inside of the global permissions database 110.

Following that, the global database 110 is queried in a step 615 and a response to the query is reformatted where necessary. The retrieved and reformatted information is then returned in a step 620 after which method 600 terminates.

Claims

1. System (100) for managing permissions of a user (165) to a plurality of services (135, 145, 155), the services having separate permissions databases (140.2, 150.2, 160.2), each permissions database holding a portion of the user's permission information, the system (100) comprising:
   - a first interface (115) for accepting a first request for accessing permissions of the user (165) to the services (135, 145, 155);
   - a repository (200) with information indicative of a first association between the user (165) and at least one user group (215) and a second association between the at least one user group (215) and access permissions to at least one of the services (135, 145, 155);
   - a processing unit (105) for determining, on the basis of the information in the repository, permissions to be set in the permissions databases (140.2, 150.2, 160.2) of the at least one service (135, 145, 155);
   - a second interface (120) for sending second requests to administration interfaces (140.4, 150.4, 160.4) of the at least one determined service (135, 145, 155) to effect access to the determined permissions.

2. System (100) according to claim 1, further comprising a global permissions database (110) for storing the determined permissions of the user (165).

3. System (100) according to claim 2, further comprising a third interface for accepting a response from at least one of the services (135, 145, 155) about whether or not said second request to the service (135, 145, 155) has been carried out, wherein the system (100) is adapted to update the user's (165) permissions in the global permissions database (110)

according to the response.

4. System (100) according to one of the previous claims, wherein the effected access to the user's (165) permissions in the service's permissions databases comprises write-only accesses.

5. System (100) according to one of the previous claims, wherein the system (100) is adapted to return, upon a corresponding request, information indicative of a plurality of users (165) who possess a predetermined access permission.

6. System (100) according to one of the previous claims, wherein the system (100) is adapted to return, upon a corresponding request, information indicative of a history of accesses to a user's (165) permissions.

7. System (100) according to one of the previous claims, wherein an administration interface (140.4, 150.4, 160.4) of one of the services (135, 145, 155) comprise an electronic mailbox (145).

8. System (100) according to one of the previous claims, wherein one of the administration interfaces (140.4, 150.4, 160.4) of the services (135, 145, 155) comprises a machine interface (370) for direct access to the user's (165) permissions on the database (140.2, 150.2, 160.2) of the service (135, 145, 155).

9. System (100) according to one of the previous claims, wherein the system (100) is adapted to reject the first request in case predefined data associated with the first request is not available to the system (100).

10. System (100) according to one of the previous claims, wherein the global permissions database (110)

is adapted to be located on a server (140, 150, 160, 305-335, 350) that is different from a server (105) on which the processing unit (105) resides.

11. System (100) according to claim 10 wherein the global permissions database (110) resides on a virtual server that is hosted on a plurality of physical servers (140, 150, 160, 305-335, 350).

12. Method (400) for managing access permissions of a user (165) to a plurality of services (135, 145, 155), the services having separate permissions databases (140.2, 150.2, 160.2), each permissions database holding a portion of the user's permission information, the method comprising steps of:
- receiving (405) a first request for accessing permissions of the user (165);
- determining (425) permissions to be set in the permissions databases of the at least one service on the basis of information indicative of a first association between the user (165) and at least one user group (215) and a second association between the at least one user group (215) and access permissions to at least one of the services;
- sending (445) second requests to administration interfaces (140.4, 150.4, 160.4) of the at least one determined service (135, 145, 155) to effect access to the determined permissions.

13. Computer program product for carrying out the method (400) of claim 12 when the computer program product is executed on a processing device (105).

14. Computer program product for carrying out the method (400) of claim 12 when the computer program product is stored on a computer-readable medium.

FIG 1

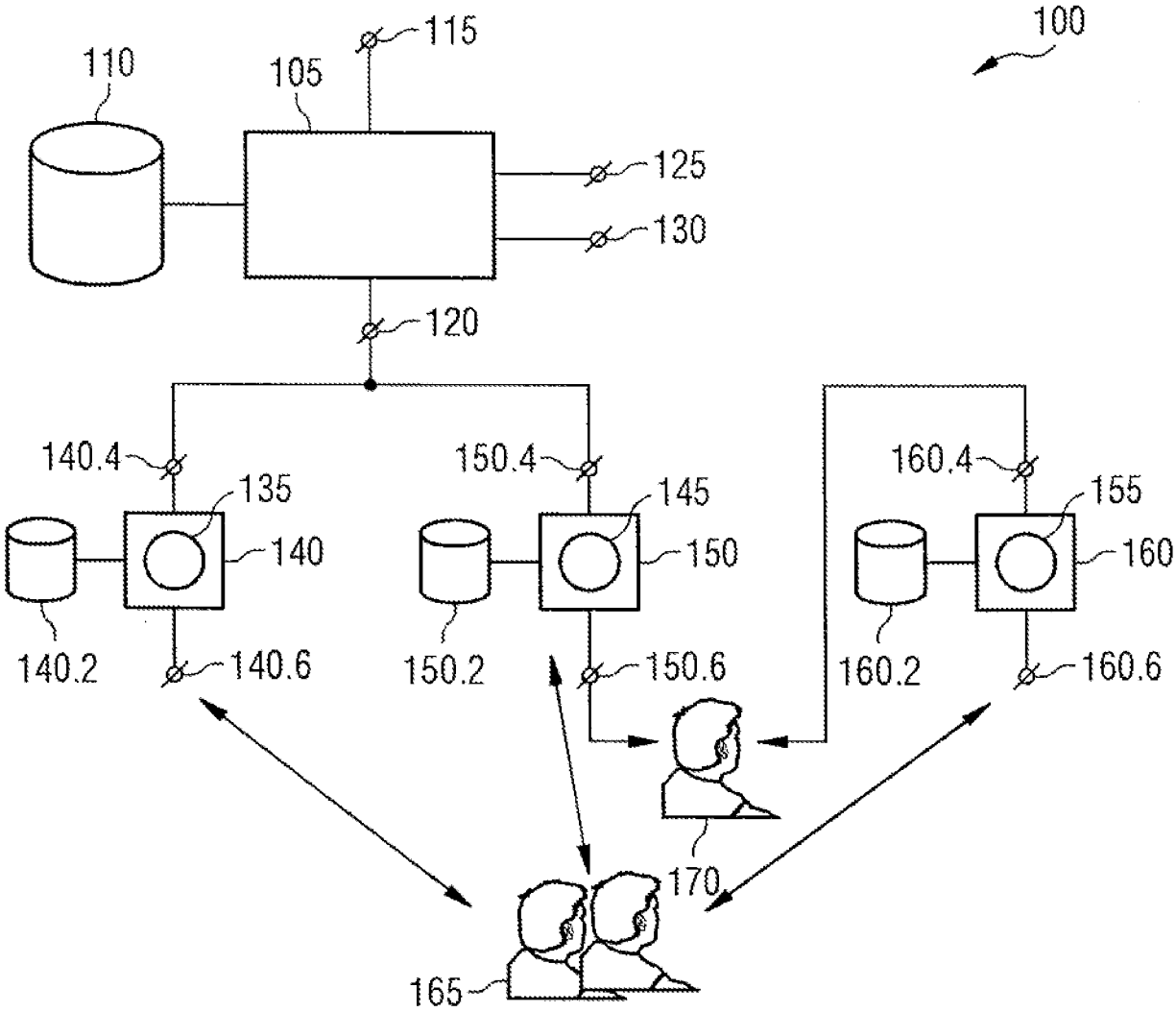
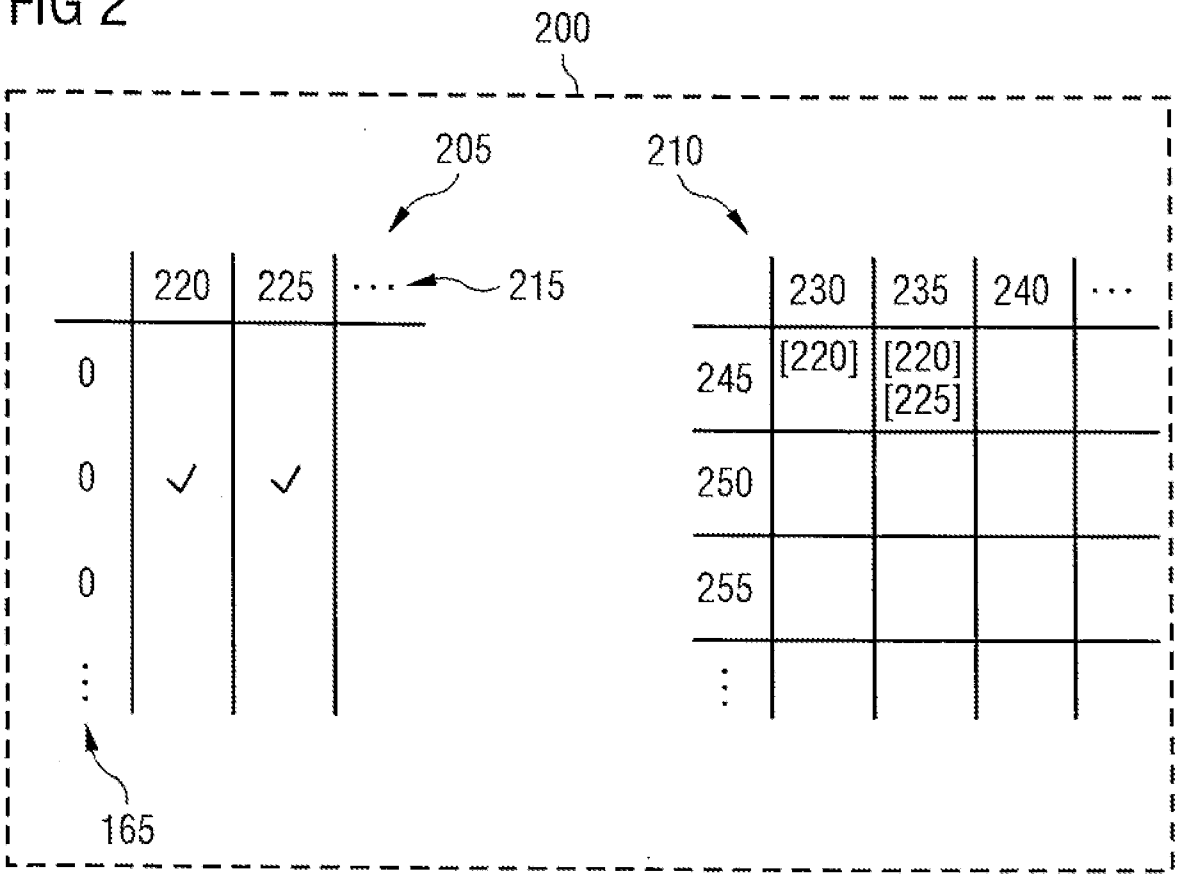

100
110
105
115
125
130
120
140.4
135
140
140.2
140.6
150.4
145
150
150.2
150.6
160.4
155
160
160.2
160.6
170
165

FIG 2


200
205
210
220
225
215
230
235
240
0
0
0
245
250
255
[220]
[220]
[225]
165

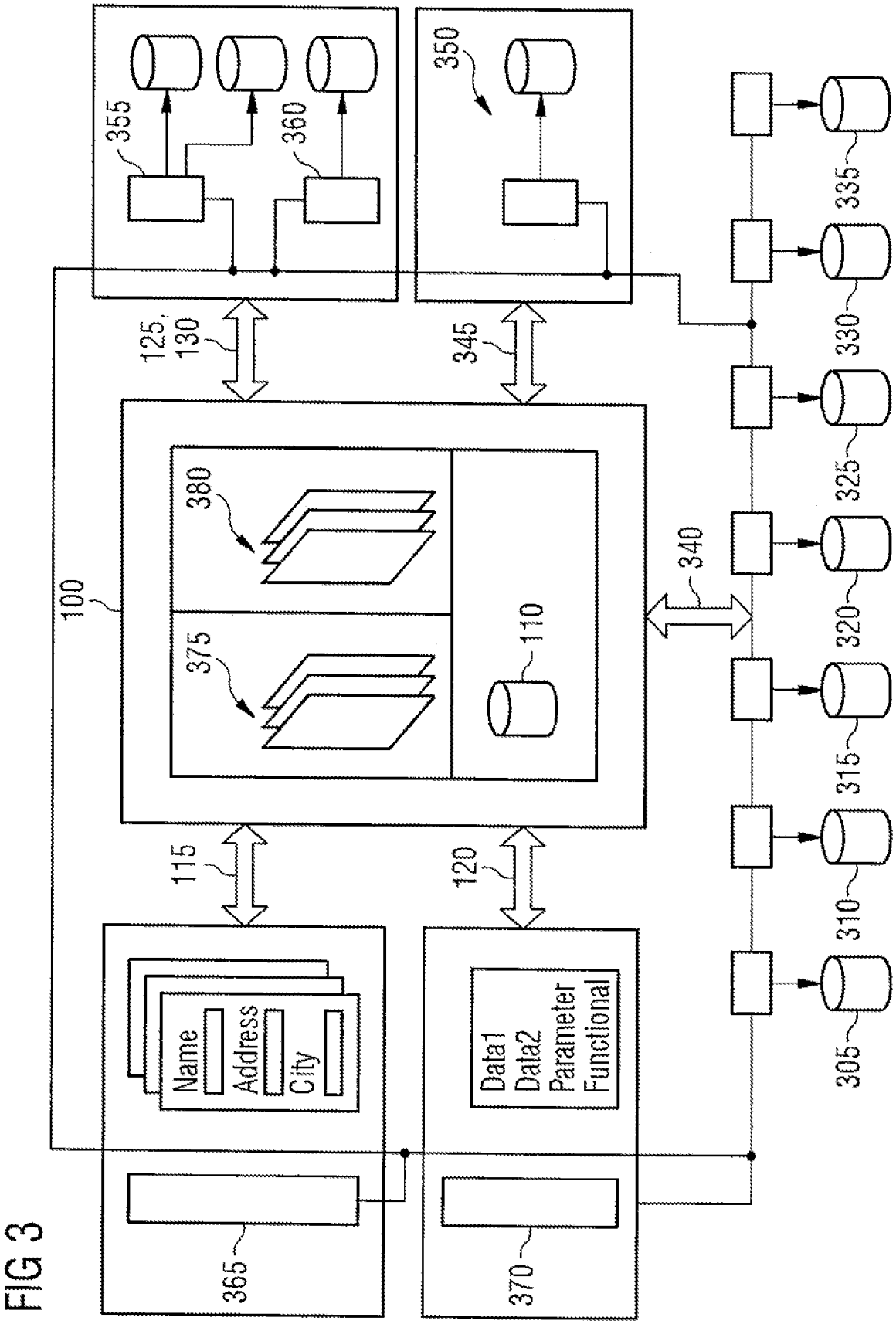

355
360
350
125, 130
345
380
375
110
100
340
115
120
Name
Address
City
Data1
Data2
Parameter
Functional
365
370
335
330
325
320
315
310
305

FIG 3

FIG 4

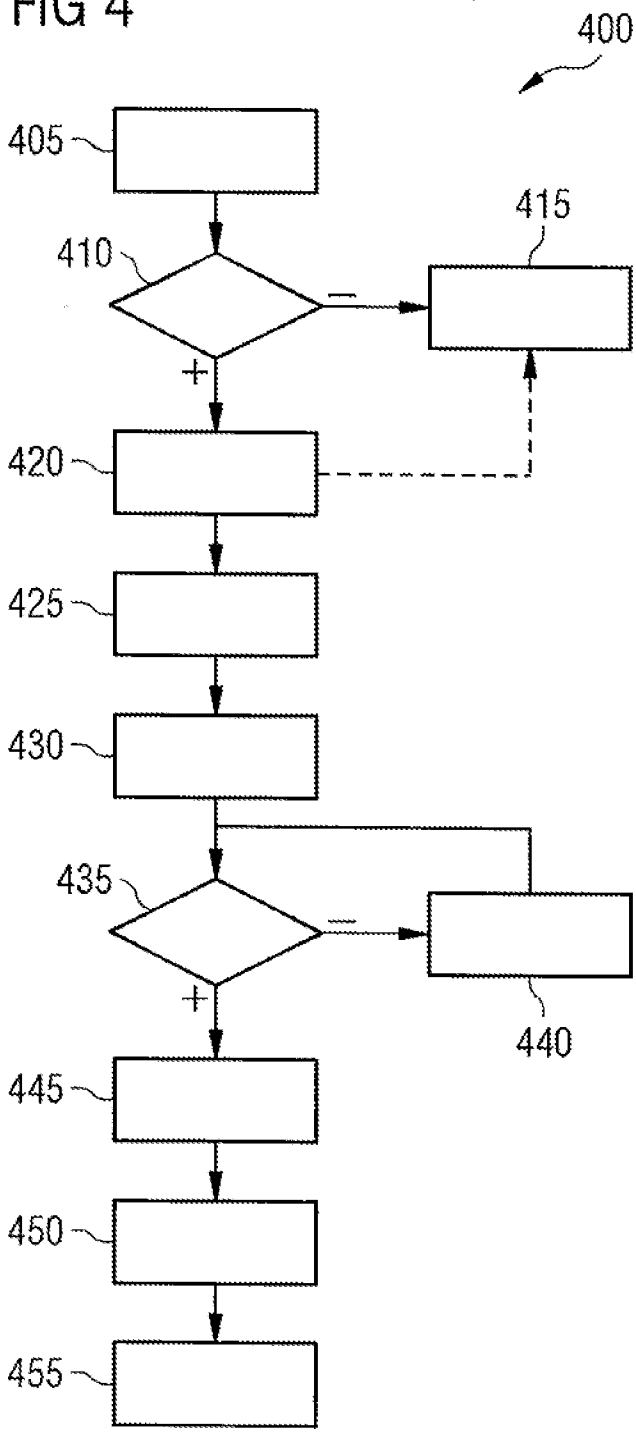


FIG 5

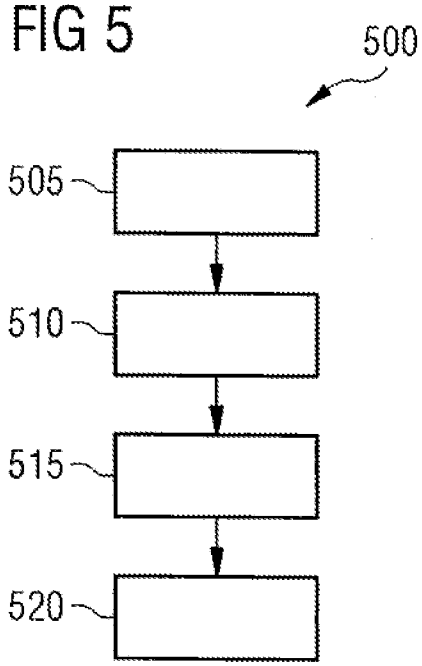
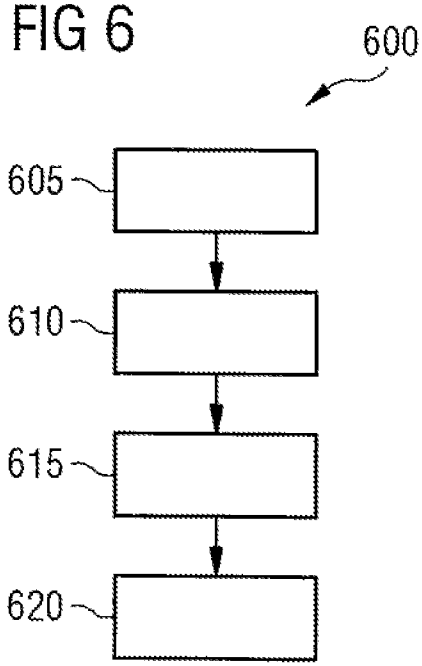


FIG 6



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2011/054538

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/24 H04L29/06
ADD.

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)
G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/078932 A1 (KAISERWERTH RUDOLF [DE] ET AL) 24 April 2003 (2003-04-24) abstract; figures 2,3 paragraph [0007] - paragraph [0008] paragraph [0014] - paragraph [0019] claims 1-9	1-14
A	US 2010/241668 A1 (SUSANTO FERRY [US] ET AL) 23 September 2010 (2010-09-23) the whole document	1-14
A	US 2002/116385 A1 (KAGALWALA RAXIT A [US] ET AL) 22 August 2002 (2002-08-22) the whole document	1-14
A	US 2006/248083 A1 (SACK PATRICK [US] ET AL) 2 November 2006 (2006-11-02) the whole document	1-14

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document 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 another 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	Date of mailing of the international search report
23 September 2011	05/10/2011

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Powell, David

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2011/054538

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003078932 A1	24-04-2003	EP 1298515 A2	02-04-2003
US 2010241668 A1	23-09-2010	NONE	
US 2002116385 A1	22-08-2002	US 2005076044 A1	07-04-2005
US 2006248083 A1	02-11-2006	NONE	