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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 August 2012 (02.08.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/101621 A1

(51) International Patent Classification:
G06F 7/04 (2006.01)

(21) International Application Number:
PCT/IL2011/000903

(22) International Filing Date:
24 November 2011 (24.11.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

13/014,762	27 January 2011 (27.01.2011)	US
61/477,662	21 April 2011 (21.04.2011)	US
13/106,023	12 May 2011 (12.05.2011)	US
13/159,903	14 June 2011 (14.06.2011)	US
13/303,826	23 November 2011 (23.11.2011)	US

(71) Applicant *(for all designated States except US)*: **VARONIS SYSTEMS, INC.** [US/US]; 23rd Floor, South Tower, 499, 7th Avenue, New York, New York 11018 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **FAITELSON, Yakov** [IL/IL]; 3 Mishol Hasapir Street, 44814 Elkana (IL). **KORKUS, Ohad** [IL/IL]; 11 Galgaley Haplada Street, 46733 Herzeliya (IL). **KRETZER-KATZIR, Ophir** [IL/IL]; 23 Tomer Street, 71799 Reut (IL).

(74) Agents: **SANFORD T. COLB & CO.** et al.; P.O. Box 2273, 76122 Rehovot (IL).

(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, QA, RO, RS, RU, RW, 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.

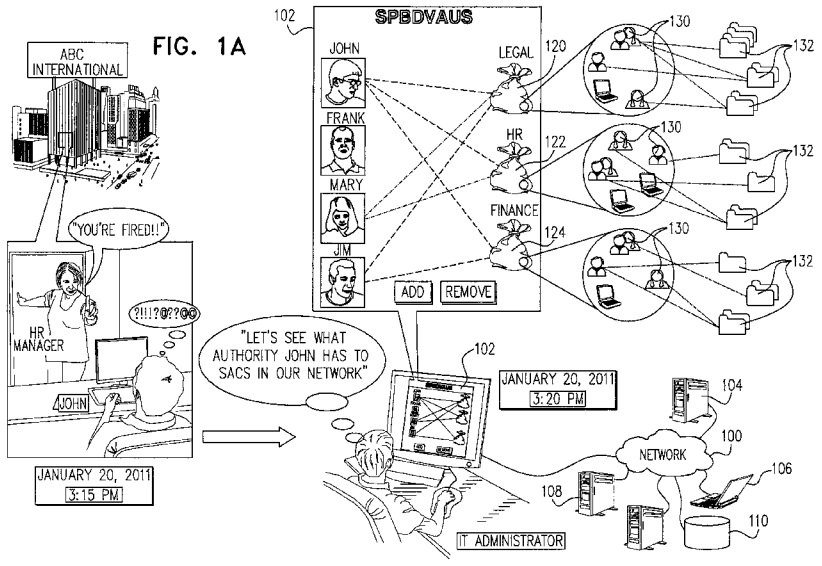
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, 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**: ACCESS PERMISSIONS MANAGEMENT SYSTEM AND METHOD

FIG. 1A



(57) **Abstract**: A system for providing bi-directional visualization of authority of users over SACs in an enterprise-wide network, the system including functionality for providing user-wise visualization of the authority of a given user over at least one SAC in respect of which the user has authority, and functionality for providing SAC-wise visualization for a given SAC of the authority of at least one user over the given SAC.

WO 2012/101621 A1

ACCESS PERMISSIONS MANAGEMENT SYSTEM AND METHOD

REFERENCE TO RELATED APPLICATIONS

Reference is made to U.S. Patent Application Serial No. 13/014,762, filed January 27, 2011, and entitled "AUTOMATIC RESOURCE OWNERSHIP ASSIGNMENT SYSTEMS AND METHODS", the disclosure of which is hereby incorporated by reference and priority of which is hereby claimed pursuant to 37 CFR 1.78(a) (1) and (2)(i).

Reference is also made to U.S. Provisional Patent Application Serial No. 61/477,662, filed April 21, 2011 and entitled "ACCESS PERMISSIONS MANAGEMENT SYSTEM AND METHOD", the disclosure of which is hereby incorporated by reference and priority of which is hereby claimed pursuant to 37 CFR 1.78(a) (4) and (5)(i).

Reference is also made to U.S. Patent Application Serial No. 13/106,023, filed May 12, 2011, and entitled "AUTOMATIC RESOURCE OWNERSHIP ASSIGNMENT SYSTEM AND METHOD", the disclosure of which is hereby incorporated by reference and priority of which is hereby claimed pursuant to 37 CFR 1.78(a) (1) and (2)(i).

Reference is also made to U.S. Patent Application Serial No. 13/159,903, filed June 14, 2011, and entitled "ACCESS PERMISSIONS MANAGEMENT SYSTEM AND METHOD", the disclosure of which is hereby incorporated by reference and priority of which is hereby claimed pursuant to 37 CFR 1.78(a) (1) and (2)(i).

Reference is also made to U.S. Patent Application Serial No. 13/303,826, filed November 23, 2011, and entitled "ACCESS PERMISSIONS MANAGEMENT SYSTEM AND METHOD", the disclosure of which is hereby incorporated by reference and priority of which is hereby claimed pursuant to 37 CFR 1.78(a) (1) and (2)(i).

Reference is also made to the following patents and patent applications, owned by assignee, the disclosures of which are hereby incorporated by reference:

U.S. Patent Nos. 7,555,482 and 7,606,801;

U.S. Published Patent Application Nos.: 2007/0244899, 2008/0271157, 2009/0100058, 2009/0119298; 2009/0265780; 2011/0010758; 2011/0060916; 2011/0061093; 2011/0061111 and 2011/0184989;

U.S. Patent Application Serial Nos.: 12/861,059; 12/861,953 and 13/106,023; 13/159,903; and 13/303,826.

PCT Applications PCT/IL2011/000409 and PCT/IL2011/000408.

FIELD OF THE INVENTION

The present invention relates to data management generally and more particularly access permissions management.

BACKGROUND OF THE INVENTION

The following patent publications are believed to represent the current state of the art:

U.S. Patent Nos.: 5,465,387; 5,899,991; 6,338,082; 6,393,468; 6,928,439; 7,031,984; 7,068,592; 7,403,925; 7,421,740; 7,555,482, 7,606,801 and 7,743,420; and

U.S. Published Patent Application Nos.: 2003/0051026; 2004/0249847; 2005/0108206; 2005/0203881; 2005/0086529; 2006/0064313; 2006/0184530; 2006/0184459; 2007/0203872; 2007/0244899; 2008/0271157; 2009/0100058; 2009/0119298 and 2009/0265780.

SUMMARY OF THE INVENTION

The present invention provides improved systems and methodologies for access permissions management.

There is thus provided in accordance with a preferred embodiment of the present invention a system for providing bi-directional visualization of authority of users over SACs in an enterprise-wide network, the system including functionality for providing user-wise visualization of the authority of a given user over at least one SAC in respect of which the user has authority, and functionality for providing SAC-wise visualization for a given SAC of the authority of at least one user over the given SAC.

The term "SAC" for the purposes of this application is defined as a container which includes network objects such as computers, user groups and printers, but which may exclude data elements such as files and file folders. The authority of a user over a SAC for the purposes of this application is defined as the ability of a user to modify properties of network objects in the SAC.

The term "network object" for the purposes of this application is defined to include enterprise computer network resources. Examples of network objects include structured and unstructured computer data resources such as files and folders, disparate users and user groups.

Preferably, the SACs do not include data elements and the functionality for providing user-wise visualization does not provide visualization of authority of a given user over data elements. Alternatively, the SACs do not include data elements and the functionality for providing user-wise visualization also provides visualization of authority of a given user over data elements. Alternatively, the SACs include data elements and the functionality for providing user-wise visualization does not provide visualization of authority of a given user over the data elements. Alternatively, the SACs include data elements and the functionality for providing user-wise visualization also provides visualization of authority of a given user over the data elements.

Preferably, the system also includes functionality for providing user-wise monitoring and reporting of the exercise of authority by a given user over at least one SAC with respect to which the user has authority, and functionality for providing SAC-

wise monitoring and reporting of the exercise of authority over a given SAC by at least one user having authority over the given SAC.

There is also provided in accordance with another preferred embodiment of the present invention a system for providing monitoring and bi-directional reporting of the exercise of authority by users and SACs in an enterprise-wide network, the system including functionality for providing user-wise monitoring and reporting of the exercise of authority by a given user over at least one SAC with respect to which the user has authority, and functionality for providing SAC-wise monitoring and reporting of the exercise of authority over a given SAC by at least one user having authority over the given SAC.

Preferably, the system also includes functionality for providing user-wise visualization of the authority of a given user over at least one SAC in respect of which the user has authority, and functionality for providing SAC-wise visualization for a given SAC of the authority of at least one user over the given SAC.

Preferably, the SACs do not include data elements and the functionality for providing user-wise visualization does not provide visualization of authority of a given user over data elements. Alternatively, the SACs do not include data elements and the functionality for providing user-wise visualization also provides visualization of authority of a given user over data elements. Alternatively, the SACs include data elements and the functionality for providing user-wise visualization does not provide visualization of authority of a given user over the data elements. Alternatively, the SACs include data elements and the functionality for providing user-wise visualization also provides visualization of authority of a given user over the data elements.

There is further provided in accordance with yet another preferred embodiment of the present invention a method for providing bi-directional visualization of authority of users over SACs in an enterprise-wide network, the method including providing user-wise visualization of the authority of a given user over at least one SAC in respect of which the user has authority, and providing SAC-wise visualization for a given SAC of the authority of at least one user over the given SAC.

Preferably, the SACs do not include data elements and providing user-wise visualization does not include providing visualization of authority of a given user over data elements. Alternatively, the SACs do not include data elements and providing

user-wise visualization also includes providing visualization of authority of a given user over data elements. Alternatively, the SACs include data elements and providing user-wise visualization does not include providing visualization of authority of a given user over the data elements. Alternatively, the SACs include data elements and providing user-wise visualization also includes providing visualization of authority of a given user over the data elements.

Preferably, the method also includes providing user-wise monitoring and reporting of the exercise of authority by a given user over at least one SAC with respect to which the user has authority, and providing SAC-wise monitoring and reporting of the exercise of authority over a given SAC by at least one user having authority over the given SAC.

There is yet further provided in accordance with still another preferred embodiment of the present invention a method for providing monitoring and bi-directional reporting of the exercise of authority by users and SACs in an enterprise-wide network, the method including providing user-wise monitoring and reporting of the exercise of authority by a given user over at least one SAC with respect to which the user has authority, and providing SAC-wise monitoring and reporting of the exercise of authority over a given SAC by at least one user having authority over the given SAC.

Preferably, the the method also includes providing user-wise visualization of the authority of a given user over at least one SAC in respect of which the user has authority, and providing SAC-wise visualization for a given SAC of the authority of at least one user over the given SAC.

Preferably, the SACs do not include data elements and providing user-wise visualization does not include providing visualization of authority of a given user over data elements. Alternatively, the SACs do not include data elements and providing user-wise visualization also includes providing visualization of authority of a given user over data elements. Alternatively, the SACs include data elements and providing user-wise visualization does not include providing visualization of authority of a given user over the data elements. Alternatively, the SACs include data elements and providing user-wise visualization also includes providing visualization of authority of a given user over the data elements.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

Figs. 1A, 1B and 1C are simplified pictorial illustrations of the use of a system for providing bi-directional visualization of authority of users over SACs in an enterprise-wide network, constructed and operative in accordance with a preferred embodiment of the present invention;

Figs. 2A, 2B and 2C are simplified pictorial illustrations of the use of a system for providing bi-directional visualization of authority of users over SACs in an enterprise-wide network, constructed and operative in accordance with another preferred embodiment of the present invention;

Figs. 3A, 3B and 3C are simplified pictorial illustrations of the use of a system for providing bi-directional visualization of authority of users over SACs in an enterprise-wide network, constructed and operative in accordance with yet another preferred embodiment of the present invention; and

Figs. 4A, 4B and 4C are simplified pictorial illustrations of the use of a system for providing bi-directional visualization of authority of users over SACs in an enterprise-wide network, constructed and operative in accordance with a further preferred embodiment of the present invention; and

Fig. 5 is a simplified block diagram illustration of the system of Figs. 1A – 4C.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Reference is now made to Figs. 1A, 1B and 1C, which are simplified pictorial illustrations of the use of a system for providing bi-directional visualization of authority of users over SACs in an enterprise-wide network, constructed and operative in accordance with a preferred embodiment of the present invention.

The term "SAC" for the purposes of this application is defined as a container which includes network objects such as computers, user groups and printers, but which may exclude data elements such as files and file folders. The authority of a user over a SAC for the purposes of this application is defined as the ability of a user to modify properties of network objects in the SAC.

The term "network object" for the purposes of this application is defined to include enterprise computer network resources. Examples of network objects include structured and unstructured computer data resources such as files and folders, disparate users and user groups.

The system for providing bi-directional visualization of authority of users over SACs (SPBDVAUS) of Figs. 1A – 1C is preferably suitable for operating in an enterprise computer environment which includes an enterprise level directory services management system which enables management of a plurality of SACs, and preferably includes functionality for providing user-wise visualization of the authority of a given user over at least one SAC in respect of which the user has authority and functionality for providing SAC-wise visualization for a given SAC of the authority of at least one user over the given SAC.

The SPBDVAUS also preferably includes functionality for providing user-wise monitoring and reporting of the exercise of authority by a given user over at least one SAC with respect to which the user has authority and functionality for providing SAC-wise monitoring and reporting of the exercise of authority over a given SAC by at least one user having authority over said given SAC.

As shown in Fig. 1A, at a particular time, such as on January 20, 2011 at 3:15 PM, an HR manager of a company notifies John, an employee of the company, that his employment with the company is terminated. Shortly thereafter, such as at 3:20 PM,

the IT manager of the enterprise network 100 of the company accesses a SPBDVAUS user interface 102 to obtain a user-wise visualization of the authority that users of network 100 have over SACs in network 100. The SPBDVAUS preferably resides on a server 104 which is preferably connected to network 100. Network 100 preferably also includes a plurality of disparate computers 106, servers 108 and storage devices 110.

As further shown in Fig. 1A, SPBDVAUS user interface 102 provides, for each of the users of network 100, user-wise visualization of the authority of a given user has over any of legal SAC 120, HR SAC 122 and finance SAC 124 of network 100. SPBDVAUS user interface 102 also provides, for each of SACs 120, 122 and 124, SAC-wise visualization for a given SAC of the authority that any of the users has over the given SAC.

As clearly shown in Fig. 1A, SACs 120, 122 and 124 do not include data elements such as files and file folders. Furthermore, user interface 102 does not provide visualization of access permissions of users included in SACs 120, 122 and 124 to data elements 132 such as files and file folders which reside on network 100.

Turning now to Fig. 1B, it is shown that the IT manager, utilizing SPBDVAUS user interface 102, ascertains that John has authority over legal SAC 120, HR SAC 122 and finance SAC 124, and immediately further utilizes user interface 102 to revoke John's authority over SACs 120, 122 and 124.

Turning now to Fig. 1C, the IT manager subsequently utilizes SPBDVAUS user interface 102 to obtain a user-wise report of the exercise of authority by John over SACs with respect to which John had authority. As seen in Fig. 1C, the IT manager ascertains that prior to termination of employment, John had granted access permissions to a legal folder to Susan, access permissions to a HR folder to Jerry and access permissions to a finance folder to Tim. The IT manager can then assess whether access permissions granted by John should be revoked.

As further shown in Fig. 1C, the IT manager utilizes SPBDVAUS user interface 102 to obtain a SAC-wise report of the exercise of authority over the legal SAC by the users having authority over the legal SAC. As seen in Fig. 1C, the IT manager ascertains that John granted access permissions to a legal folder to Susan, that Mary granted access permissions to a legal folder to Ron, and that Jim granted access permissions to a legal folder to David.

Reference is now made to Figs. 2A, 2B and 2C, which are simplified pictorial illustrations of the use of a system for providing bi-directional visualization of authority of users over SACs in an enterprise-wide network, constructed and operative in accordance with another preferred embodiment of the present invention.

The system for providing bi-directional visualization of authority of users over SACs (SPBDVAUS) of Figs. 2A - 2C is preferably suitable for operating in an enterprise computer environment which includes an enterprise level directory services management system which enables management of a plurality of SACs, and preferably includes functionality for providing user-wise visualization of the authority of a given user over at least one SAC in respect of which the user has authority and functionality for providing SAC-wise visualization for a given SAC of the authority of at least one user over the given SAC.

The SPBDVAUS also preferably includes functionality for providing user-wise monitoring and reporting of the exercise of authority by a given user over at least one SAC with respect to which the user has authority and functionality for providing SAC-wise monitoring and reporting of the exercise of authority over a given SAC by at least one user having authority over said given SAC.

As shown in Fig. 2A, at a particular time, such as on January 20, 2011 at 3:15 PM, an HR manager of a company notifies John, an employee of the company, that his employment with the company is terminated. Shortly thereafter, such as at 3:20 PM, the IT manager of the enterprise network 200 of the company accesses a SPBDVAUS user interface 202 to obtain a user-wise visualization of the authority that users of network 200 have over SACs in network 200. The SPBDVAUS preferably resides on a server 204 which is preferably connected to network 200. Network 200 preferably also includes a plurality of disparate computers 206, servers 208 and storage devices 210.

As further shown in Fig. 2A, SPBDVAUS user interface 202 provides, for each of the users of network 220, user-wise visualization of the authority of a given user has over any of legal SAC 220, HR SAC 222 and finance SAC 224 of network 200. SPBDVAUS user interface 202 also provides, for each of SACs 220, 222 and 224, SAC-wise visualization for a given SAC of the authority that any of the users has over the given SAC.

As clearly shown in Fig. 2A, SACs 220, 222 and 224 do not include data elements such as files and file folders. However, user interface 202 provides visualization of access permissions of users included in SACs 220, 222 and 224 to data elements 232 such as files and file folders which reside on network 200.

Turning now to Fig. 2B, it is shown that the IT manager, utilizing SPBDVAUS user interface 202, ascertains that John has authority over legal SAC 220, HR SAC 222 and finance SAC 224, and immediately further utilizes user interface 202 to revoke John's authority over SACs 220, 222 and 224.

Turning now to Fig. 2C, the IT manager subsequently utilizes SPBDVAUS user interface 202 to obtain a user-wise report of the exercise of authority by John over SACs with respect to which John had authority. As seen in Fig. 2C, the IT manager ascertains that prior to termination of employment, John had granted access permissions to a legal folder to Susan, access permissions to a HR folder to Jerry and access permissions to a finance folder to Tim. The IT manager can then assess whether access permissions granted by John should be revoked.

As further shown in Fig. 2C, the IT manager utilizes SPBDVAUS user interface 202 to obtain a SAC-wise report of the exercise of authority over the legal SAC by the users having authority over the legal SAC. As seen in Fig. 2C, the IT manager ascertains that John granted access permissions to a legal folder to Susan, that Mary granted access permissions to a legal folder to Ron, and that Jim granted access permissions to a legal folder to David.

Reference is now made to Figs. 3A, 3B and 3C, which are simplified pictorial illustrations of the use of a system for providing bi-directional visualization of authority of users over SACs in an enterprise-wide network, constructed and operative in accordance with yet another preferred embodiment of the present invention.

The system for providing bi-directional visualization of authority of users over SACs (SPBDVAUS) of Figs. 3A – 3C is preferably suitable for operating in an enterprise computer environment which includes an enterprise level directory services management system which enables management of a plurality of SACs, and preferably includes functionality for providing user-wise visualization of the authority of a given user over at least one SAC in respect of which the user has authority and functionality

for providing SAC-wise visualization for a given SAC of the authority of at least one user over the given SAC.

The SPBDVAUS also preferably includes functionality for providing user-wise monitoring and reporting of the exercise of authority by a given user over at least one SAC with respect to which the user has authority and functionality for providing SAC-wise monitoring and reporting of the exercise of authority over a given SAC by at least one user having authority over said given SAC.

As shown in Fig. 3A, at a particular time, such as on January 20, 2011 at 3:15 PM, an HR manager of a company notifies John, an employee of the company, that his employment with the company is terminated. Shortly thereafter, such as at 3:20 PM, the IT manager of the enterprise network 300 of the company accesses a SPBDVAUS user interface 302 to obtain a user-wise visualization of the authority that users of network 300 have over SACs in network 300. The SPBDVAUS preferably resides on a server 304 which is preferably connected to network 300. Network 300 preferably also includes a plurality of disparate computers 306, servers 308 and storage devices 310.

As further shown in Fig. 3A, SPBDVAUS user interface 302 provides, for each of the users of network 320, user-wise visualization of the authority of a given user has over any of legal SAC 320, HR SAC 322 and finance SAC 324 of network 300. SPBDVAUS user interface 302 also provides, for each of SACs 320, 322 and 324, SAC-wise visualization for a given SAC of the authority that any of the users has over the given SAC.

As clearly shown in Fig. 3A, SACs 320, 322 and 324 include data elements 332 such as files and file folders. However, user interface 302 does not provide visualization of access permissions of users included in SACs 320, 322 and 324 to data elements 332 such as files and file folders which reside on network 300.

Turning now to Fig. 3B, it is shown that the IT manager, utilizing SPBDVAUS user interface 302, ascertains that John has authority over legal SAC 320, HR SAC 322 and finance SAC 324, and immediately further utilizes user interface 302 to revoke John's authority over SACs 320, 322 and 324.

Turning now to Fig. 3C, the IT manager subsequently utilizes SPBDVAUS user interface 302 to obtain a user-wise report of the exercise of authority by John over SACs with respect to which John had authority. As seen in Fig. 3C, the IT

manager ascertains that prior to termination of employment, John had granted access permissions to a legal folder to Susan, access permissions to a HR folder to Jerry and access permissions to a finance folder to Tim. The IT manager can then assess whether access permissions granted by John should be revoked.

As further shown in Fig. 3C, the IT manager utilizes SPBDVAUS user interface 302 to obtain a SAC-wise report of the exercise of authority over the legal SAC by the users having authority over the legal SAC. As seen in Fig. 3C, the IT manager ascertains that John granted access permissions to a legal folder to Susan, that Mary granted access permissions to a legal folder to Ron, and that Jim granted access permissions to a legal folder to David.

Reference is now made to Figs. 4A, 4B and 4C, which are simplified pictorial illustrations of the use of a system for providing bi-directional visualization of authority of users over SACs in an enterprise-wide network, constructed and operative in accordance with yet another preferred embodiment of the present invention.

The system for providing bi-directional visualization of authority of users over SACs (SPBDVAUS) of Figs. 4A – 4C is preferably suitable for operating in an enterprise computer environment which includes an enterprise level directory services management system which enables management of a plurality of SACs, and preferably includes functionality for providing user-wise visualization of the authority of a given user over at least one SAC in respect of which the user has authority and functionality for providing SAC-wise visualization for a given SAC of the authority of at least one user over the given SAC.

The SPBDVAUS also preferably includes functionality for providing user-wise monitoring and reporting of the exercise of authority by a given user over at least one SAC with respect to which the user has authority and functionality for providing SAC-wise monitoring and reporting of the exercise of authority over a given SAC by at least one user having authority over said given SAC.

As shown in Fig. 4A, at a particular time, such as on January 20, 2011 at 3:15 PM, an HR manager of a company notifies John, an employee of the company, that his employment with the company is terminated. Shortly thereafter, such as at 3:20 PM, the IT manager of the enterprise network 400 of the company accesses a SPBDVAUS user interface 402 to obtain a user-wise visualization of the authority that users of

network 400 have over SACs in network 400. The SPBDVAUS preferably resides on a server 404 which is preferably connected to network 400. Network 400 preferably also includes a plurality of disparate computers 406, servers 408 and storage devices 410.

As further shown in Fig. 4A, SPBDVAUS user interface 402 provides, for each of the users of network 420, user-wise visualization of the authority of a given user has over any of legal SAC 420, HR SAC 422 and finance SAC 424 of network 400. SPBDVAUS user interface 402 also provides, for each of SACs 420, 422 and 424, SAC-wise visualization for a given SAC of the authority that any of the users has over the given SAC.

As clearly shown in Fig. 4A, SACs 420, 422 and 424 include data elements 432 such as files and file folders. Furthermore, user interface 402 provides visualization of access permissions of users included in SACs 420, 422 and 424 to data elements 432 such as files and file folders which reside on network 400.

Turning now to Fig. 4B, it is shown that the IT manager, utilizing SPBDVAUS user interface 402, ascertains that John has authority over legal SAC 420, HR SAC 422 and finance SAC 424, and immediately further utilizes user interface 402 to revoke John's authority over SACs 420, 422 and 424.

Turning now to Fig. 4C, the IT manager subsequently utilizes SPBDVAUS user interface 402 to obtain a user-wise report of the exercise of authority by John over SACs with respect to which John had authority. As seen in Fig. 4C, the IT manager ascertains that prior to termination of employment, John had granted access permissions to a legal folder to Susan, access permissions to a HR folder to Jerry and access permissions to a finance folder to Tim. The IT manager can then assess whether access permissions granted by John should be revoked.

As further shown in Fig. 4C, the IT manager utilizes SPBDVAUS user interface 402 to obtain a SAC-wise report of the exercise of authority over the legal SAC by the users having authority over the legal SAC. As seen in Fig. 4C, the IT manager ascertains that John granted access permissions to a legal folder to Susan, that Mary granted access permissions to a legal folder to Ron, and that Jim granted access permissions to a legal folder to David.

Reference is now made to Fig. 5, which is a simplified block diagram illustration of the system of Figs. 1A – 4C. As shown in Fig. 5, the SPBDVAUS 500

preferably includes user-wise visualization functionality 502 for providing user-wise visualization of the authority of a given user over at least one SAC in respect of which the user has authority and SAC-wise visualization functionality 504 for providing SAC-wise visualization for a given SAC of the authority of at least one user over the given SAC.

SPBDVAUS 500 also preferably includes user-wise monitoring and reporting functionality 506 for providing user-wise monitoring and reporting of the exercise of authority by a given user over at least one SAC with respect to which the user has authority, and SAC-wise monitoring and reporting functionality 508 for providing SAC-wise monitoring and reporting of the exercise of authority over a given SAC by at least one user having authority over said given SAC.

It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather, the invention also includes various combinations and subcombinations of the features described hereinabove as well as modifications and variations thereof, which would occur to persons skilled in the art upon reading the foregoing and which are not in the prior art.

CLAIMS

1. A system for providing bi-directional visualization of authority of users over SACs in an enterprise-wide network, the system comprising:

functionality for providing user-wise visualization of the authority of a given user over at least one SAC in respect of which the user has authority; and

functionality for providing SAC-wise visualization for a given SAC of the authority of at least one user over said given SAC.

2. A system according to claim 1 and wherein:

said SACs do not include data elements; and

said functionality for providing user-wise visualization does not provide visualization of authority of a given user over data elements.

3. A system according to claim 1 and wherein:

said SACs do not include data elements; and

said functionality for providing user-wise visualization also provides visualization of authority of a given user over data elements.

4. A system according to claim 1 and wherein:

said SACs include data elements; and

said functionality for providing user-wise visualization does not provide visualization of authority of a given user over said data elements.

5. A system according to claim 1 and wherein:

said SACs include data elements; and

said functionality for providing user-wise visualization also provides visualization of authority of a given user over said data elements.

6. A system according to any of claims 1 - 5 and also comprising:

functionality for providing user-wise monitoring and reporting of the exercise of authority by a given user over at least one SAC with respect to which the user has authority; and

functionality for providing SAC-wise monitoring and reporting of the exercise of authority over a given SAC by at least one user having authority over said given SAC.

7. A system for providing monitoring and bi-directional reporting of the exercise of authority by users and SACs in an enterprise-wide network, the system comprising:

functionality for providing user-wise monitoring and reporting of the exercise of authority by a given user over at least one SAC with respect to which the user has authority; and

functionality for providing SAC-wise monitoring and reporting of the exercise of authority over a given SAC by at least one user having authority over said given SAC.

8. A system according to claim 7 and also comprising:

functionality for providing user-wise visualization of the authority of a given user over at least one SAC in respect of which the user has authority; and

functionality for providing SAC-wise visualization for a given SAC of the authority of at least one user over said given SAC.

9. A system according to claim 8 and wherein:

said SACs do not include data elements; and

said functionality for providing user-wise visualization does not provide visualization of authority of a given user over data elements.

10. A system according to claim 8 and wherein:

said SACs do not include data elements; and

said functionality for providing user-wise visualization also provides visualization of authority of a given user over data elements.

11. A system according to claim 8 and wherein:

said SACs include data elements; and

said functionality for providing user-wise visualization does not provide visualization of authority of a given user over said data elements.

12. A system according to claim 8 and wherein:

said SACs include data elements; and

said functionality for providing user-wise visualization also provides visualization of authority of a given user over said data elements.

13. A method for providing bi-directional visualization of authority of users over SACs in an enterprise-wide network, the method comprising:

providing user-wise visualization of the authority of a given user over at least one SAC in respect of which the user has authority; and

providing SAC-wise visualization for a given SAC of the authority of at least one user over said given SAC.

14. A method according to claim 13 and wherein:

said SACs do not include data elements; and

said providing user-wise visualization does not include providing visualization of authority of a given user over data elements.

15. A method according to claim 13 and wherein:

said SACs do not include data elements; and

said providing user-wise visualization also includes providing visualization of authority of a given user over data elements.

16. A method according to claim 13 and wherein:

said SACs include data elements; and

said providing user-wise visualization does not include providing visualization of authority of a given user over said data elements.

17. A method according to claim 13 and wherein:

said SACs include data elements; and

said providing user-wise visualization also includes providing visualization of authority of a given user over said data elements.

18. A method according to any of claims 13 - 17 and also comprising:

providing user-wise monitoring and reporting of the exercise of authority by a given user over at least one SAC with respect to which the user has authority; and

providing SAC-wise monitoring and reporting of the exercise of authority over a given SAC by at least one user having authority over said given SAC.

19. A method for providing monitoring and bi-directional reporting of the exercise of authority by users and SACs in an enterprise-wide network, the method comprising:

providing user-wise monitoring and reporting of the exercise of authority by a given user over at least one SAC with respect to which the user has authority; and

providing SAC-wise monitoring and reporting of the exercise of authority over a given SAC by at least one user having authority over said given SAC.

20. A method according to claim 19 and also comprising:

providing user-wise visualization of the authority of a given user over at least one SAC in respect of which the user has authority; and

providing SAC-wise visualization for a given SAC of the authority of at least one user over said given SAC.

21. A method according to claim 20 and wherein:

said SACs do not include data elements; and

said providing user-wise visualization does not include providing visualization of authority of a given user over data elements.

22. A method according to claim 20 and wherein:

said SACs do not include data elements; and

said providing user-wise visualization also includes providing visualization of authority of a given user over data elements.

23. A method according to claim 20 and wherein:

said SACs include data elements; and

said providing user-wise visualization does not include providing visualization of authority of a given user over said data elements.

24. A method according to claim 20 and wherein:

said SACs include data elements; and

said providing user-wise visualization also includes providing visualization of authority of a given user over said data elements.

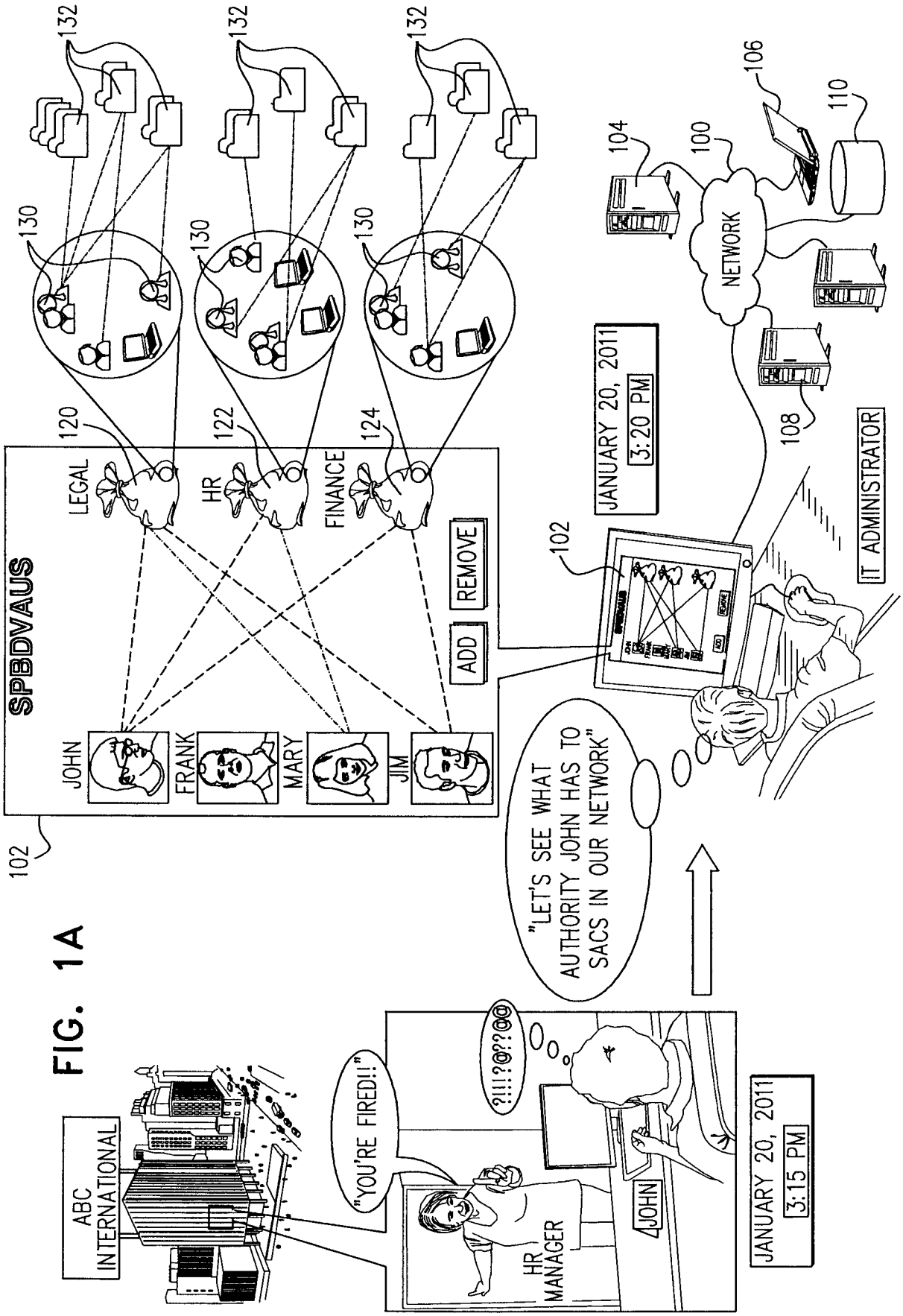

SPBDVAUS
LEGAL
HR
FINANCE
JOHN
FRANK
MARY
JIM
ADD
REMOVE
102
120
122
124
130
132
NETWORK
104
100
106
110
108
JANUARY 20, 2011
3:20 PM
IT ADMINISTRATOR
"LET'S SEE WHAT AUTHORITY JOHN HAS TO SACS IN OUR NETWORK"
ABC INTERNATIONAL
"YOU'RE FIRED!!"
?!!!?@??@@
HR MANAGER
JOHN
JANUARY 20, 2011
3:15 PM

FIG. 1A

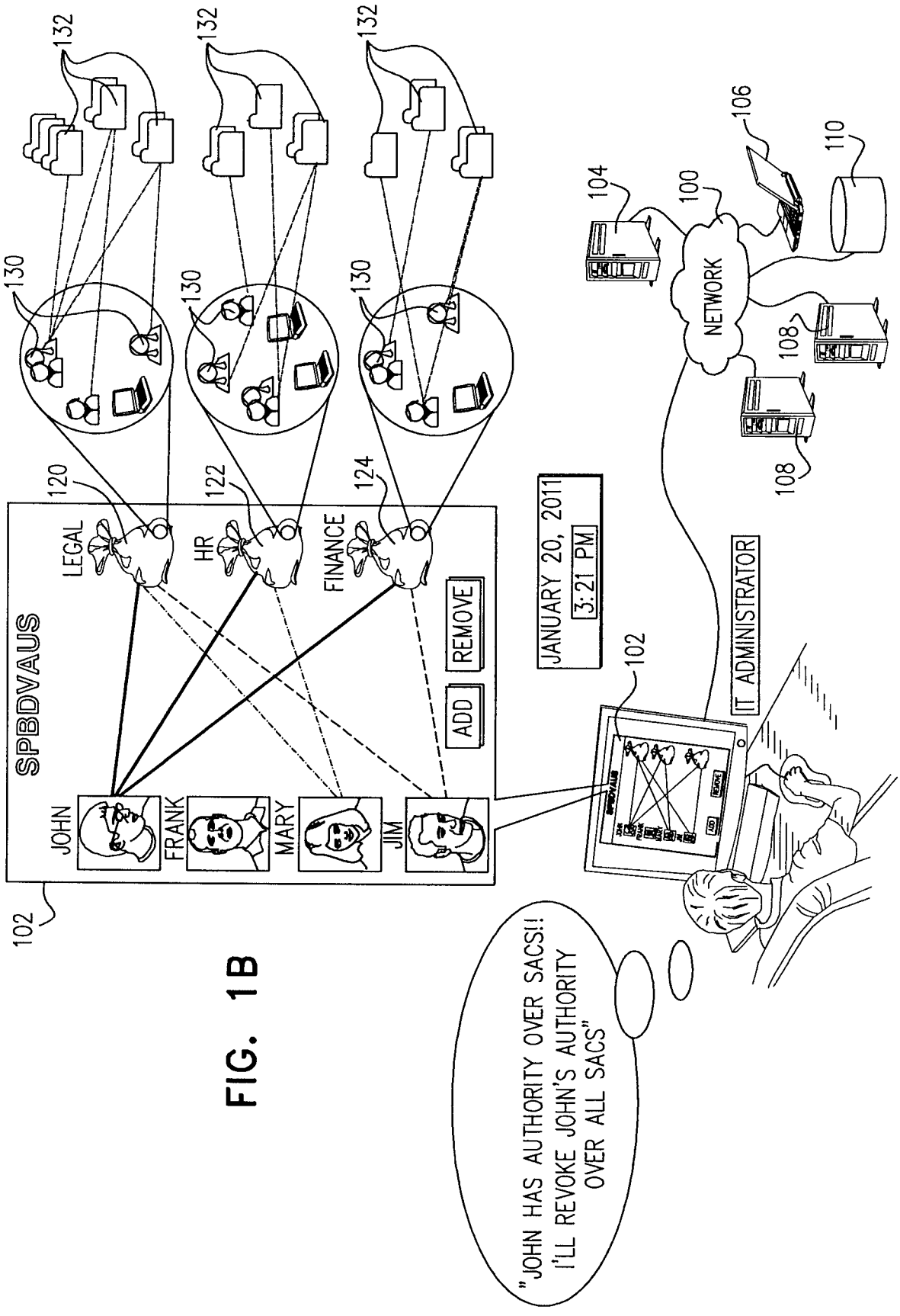
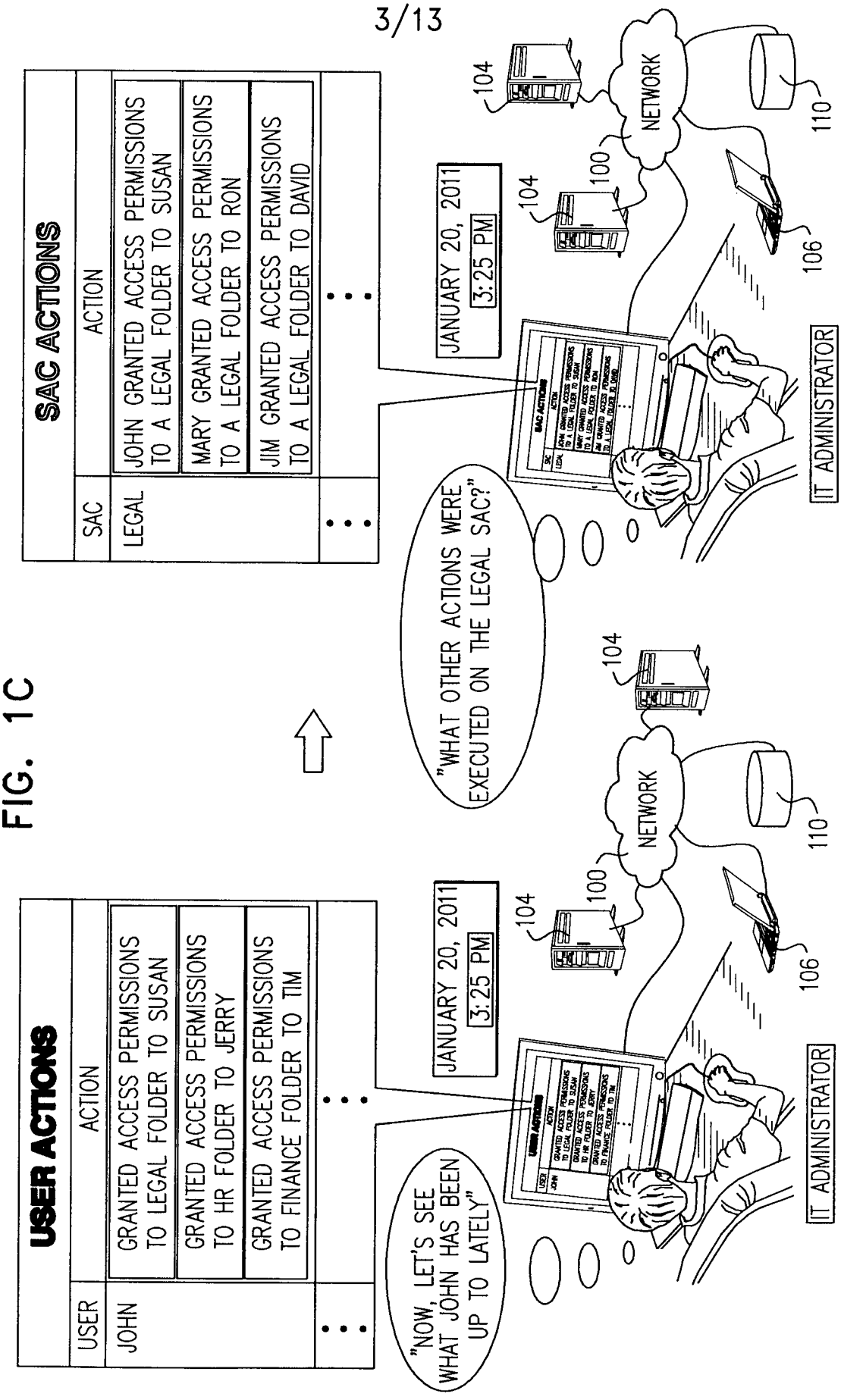

132
132
132
130
130
130
120
122
124
LEGAL
HR
FINANCE
SPBDVAUS
JOHN
FRANK
MARY
JIM
ADD
REMOVE
102
JANUARY 20, 2011
3:21 PM
102
IT ADMINISTRATOR
104
100
NETWORK
106
110
108
108
"JOHN HAS AUTHORITY OVER SACS!!
I'LL REVOKE JOHN'S AUTHORITY
OVER ALL SACS"

FIG. 1B

FIG. 1C


USER ACTIONS
USER
ACTION
JOHN
GRANTED ACCESS PERMISSIONS TO LEGAL FOLDER TO SUSAN
GRANTED ACCESS PERMISSIONS TO HR FOLDER TO JERRY
GRANTED ACCESS PERMISSIONS TO FINANCE FOLDER TO TIM
"NOW, LET'S SEE WHAT JOHN HAS BEEN UP TO LATELY"
JANUARY 20, 2011
3:25 PM
SAC ACTIONS
SAC
ACTION
LEGAL
JOHN GRANTED ACCESS PERMISSIONS TO A LEGAL FOLDER TO SUSAN
MARY GRANTED ACCESS PERMISSIONS TO A LEGAL FOLDER TO RON
JIM GRANTED ACCESS PERMISSIONS TO A LEGAL FOLDER TO DAVID
"WHAT OTHER ACTIONS WERE EXECUTED ON THE LEGAL SAC?"
JANUARY 20, 2011
3:25 PM
NETWORK
100
104
106
110
IT ADMINISTRATOR

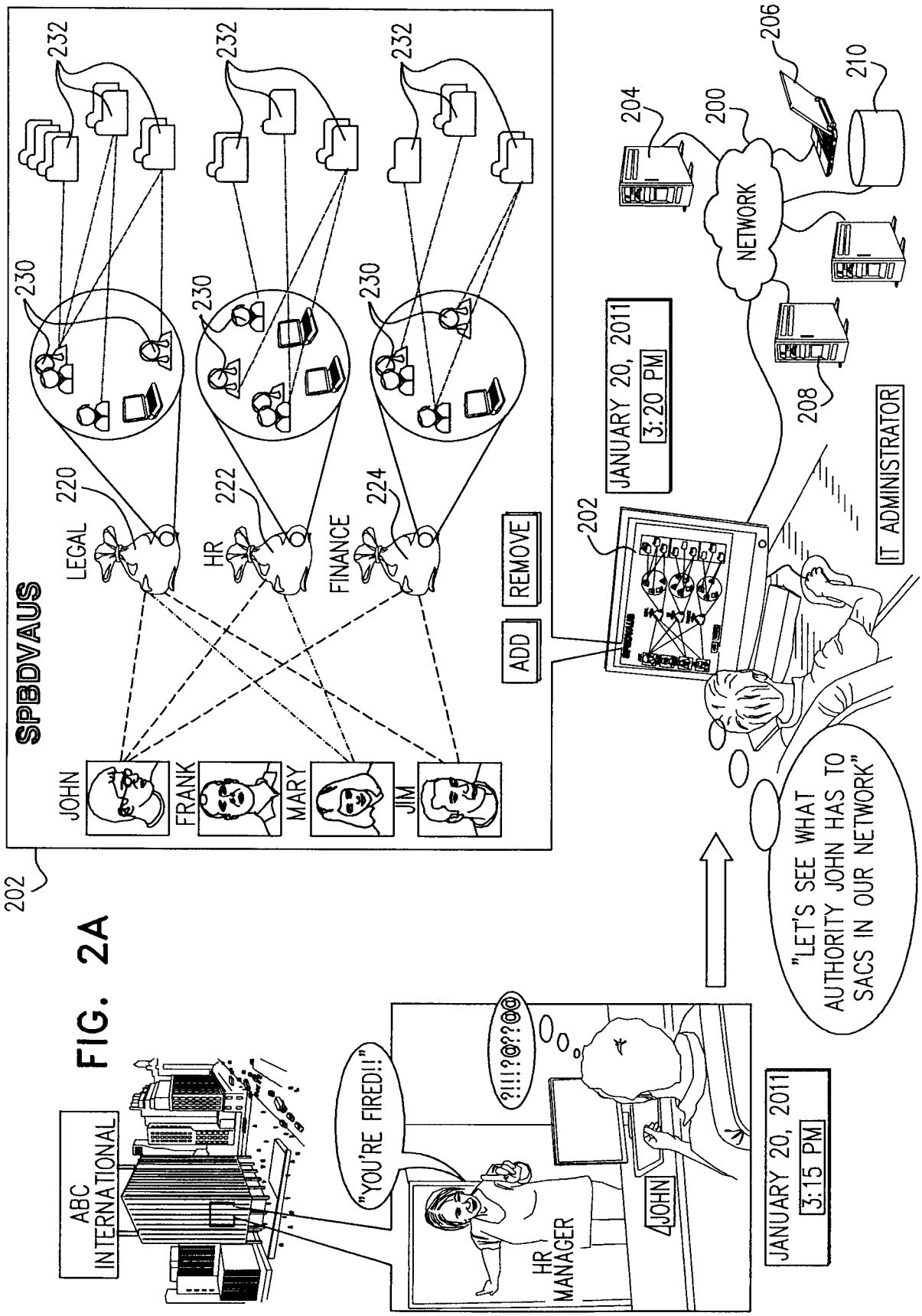

SPBDVAUS
LEGAL
HR
FINANCE
220
222
224
230
232
JOHN
FRANK
MARY
JIM
ADD
REMOVE
202
NETWORK
200
204
206
208
210
JANUARY 20, 2011
3:20 PM
IT ADMINISTRATOR
"LET'S SEE WHAT AUTHORITY JOHN HAS TO SACS IN OUR NETWORK"
ABC INTERNATIONAL
"YOU'RE FIRED!!"
?!!!?@??@@
HR MANAGER
JOHN
JANUARY 20, 2011
3:15 PM

FIG. 2A

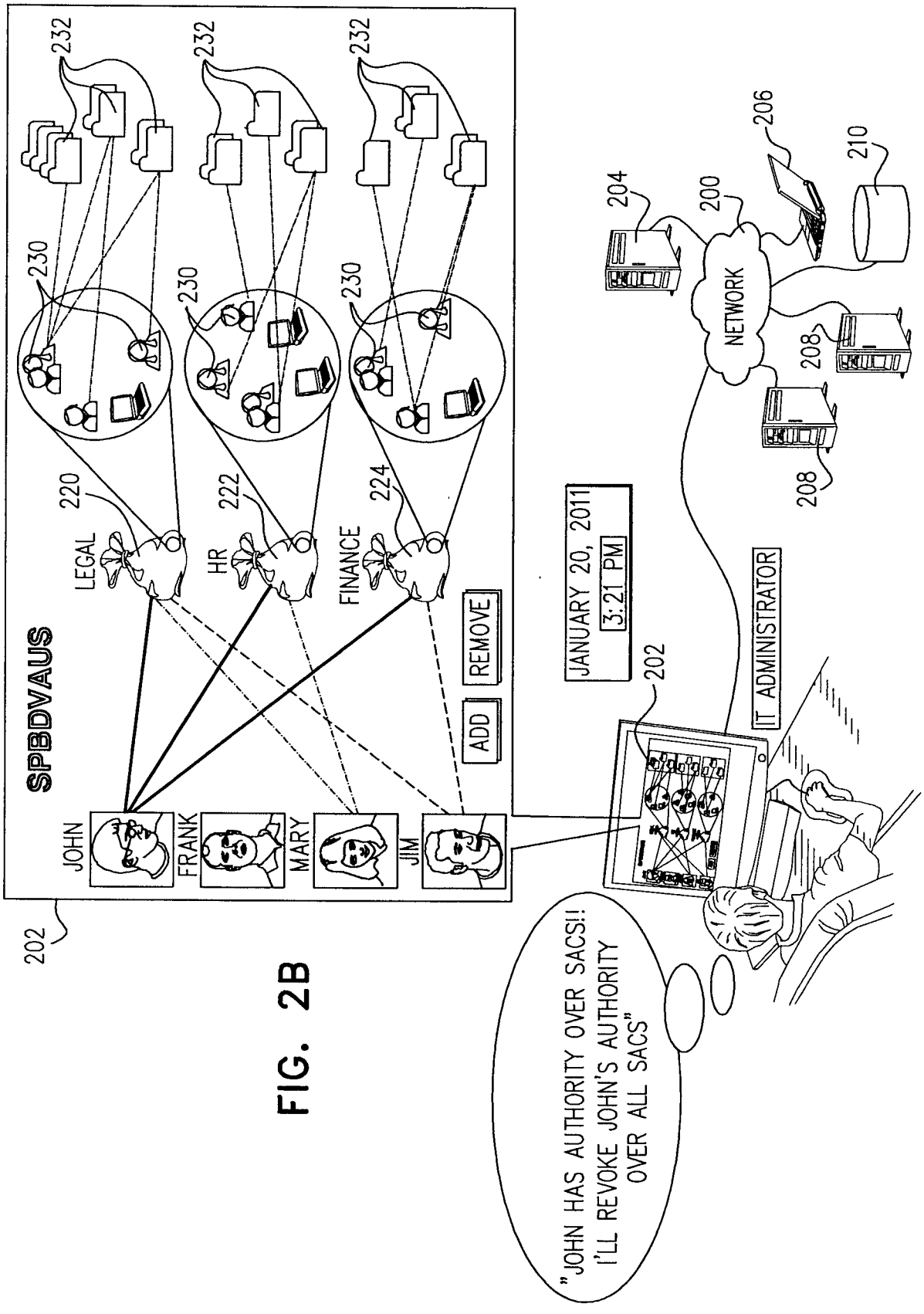

SPBDVAUS
232
230
220
LEGAL
222
HR
224
FINANCE
JOHN
FRANK
MARY
JIM
ADD
REMOVE
202
JANUARY 20, 2011
3:21 PM
IT ADMINISTRATOR
"JOHN HAS AUTHORITY OVER SACS!!
I'LL REVOKE JOHN'S AUTHORITY
OVER ALL SACS"
NETWORK
204
200
206
210
208

FIG. 2B

FIG. 2C

USER ACTIONS
USER
ACTION
JOHN
GRANTED ACCESS PERMISSIONS TO LEGAL FOLDER TO SUSAN
GRANTED ACCESS PERMISSIONS TO HR FOLDER TO JERRY
GRANTED ACCESS PERMISSIONS TO FINANCE FOLDER TO TIM
"NOW, LET'S SEE WHAT JOHN HAS BEEN UP TO LATELY"
JANUARY 20, 2011 3:25 PM
SAC ACTIONS
SAC
ACTION
LEGAL
JOHN GRANTED ACCESS PERMISSIONS TO A LEGAL FOLDER TO SUSAN
MARY GRANTED ACCESS PERMISSIONS TO A LEGAL FOLDER TO RON
JIM GRANTED ACCESS PERMISSIONS TO A LEGAL FOLDER TO DAVID
"WHAT OTHER ACTIONS WERE EXECUTED ON THE LEGAL SAC?"
JANUARY 20, 2011 3:25 PM
NETWORK
200
204
206
210
IT ADMINISTRATOR

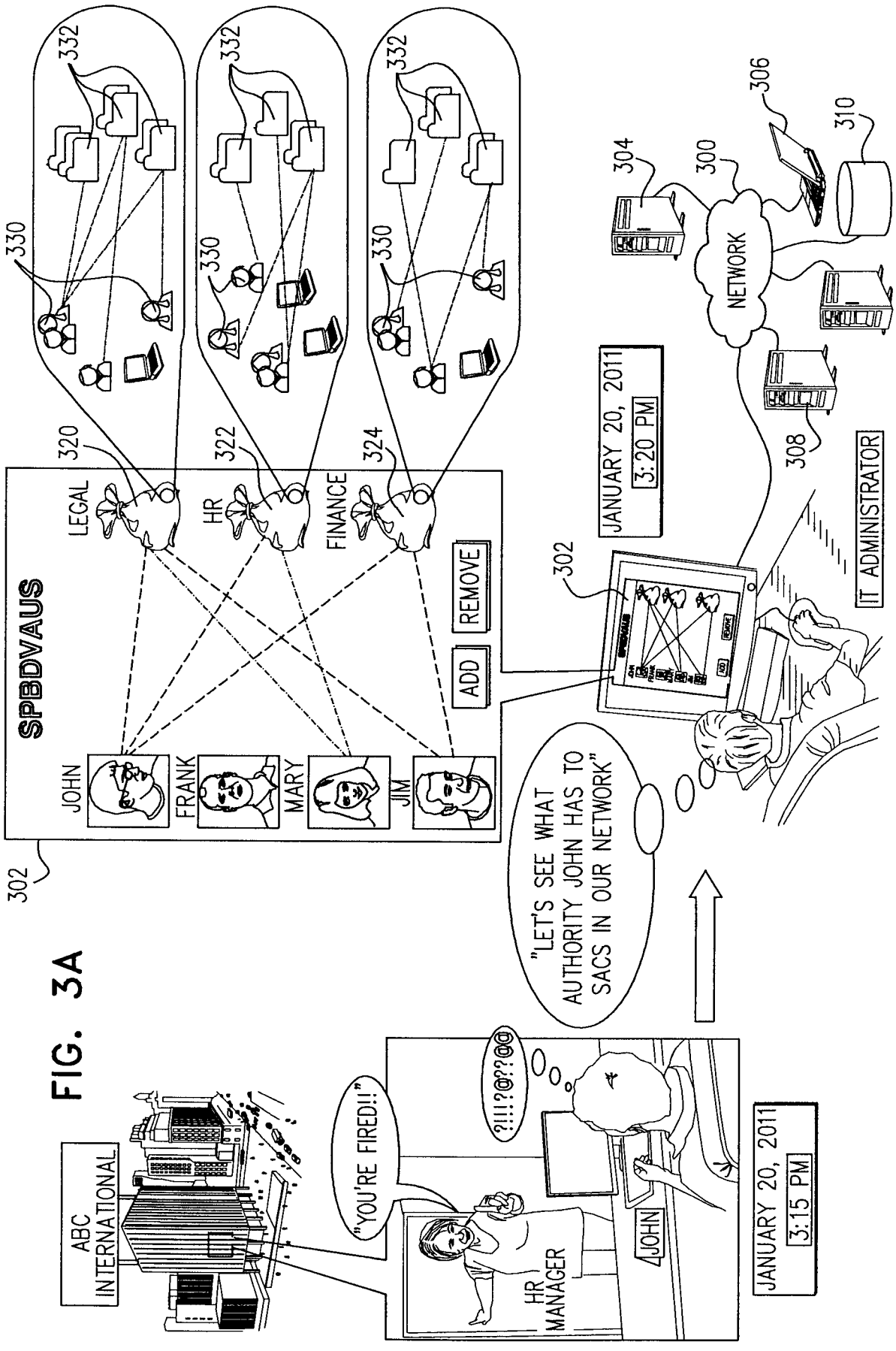

SPBDVAUS
LEGAL
HR
FINANCE
320
322
324
330
332
JOHN
FRANK
MARY
JIM
ADD
REMOVE
302
JANUARY 20, 2011
3:20 PM
NETWORK
304
300
306
310
308
IT ADMINISTRATOR
"LET'S SEE WHAT AUTHORITY JOHN HAS TO SACS IN OUR NETWORK"
ABC INTERNATIONAL
"YOU'RE FIRED!!"
?!!!?@??@@
HR MANAGER
JOHN
JANUARY 20, 2011
3:15 PM

FIG. 3A

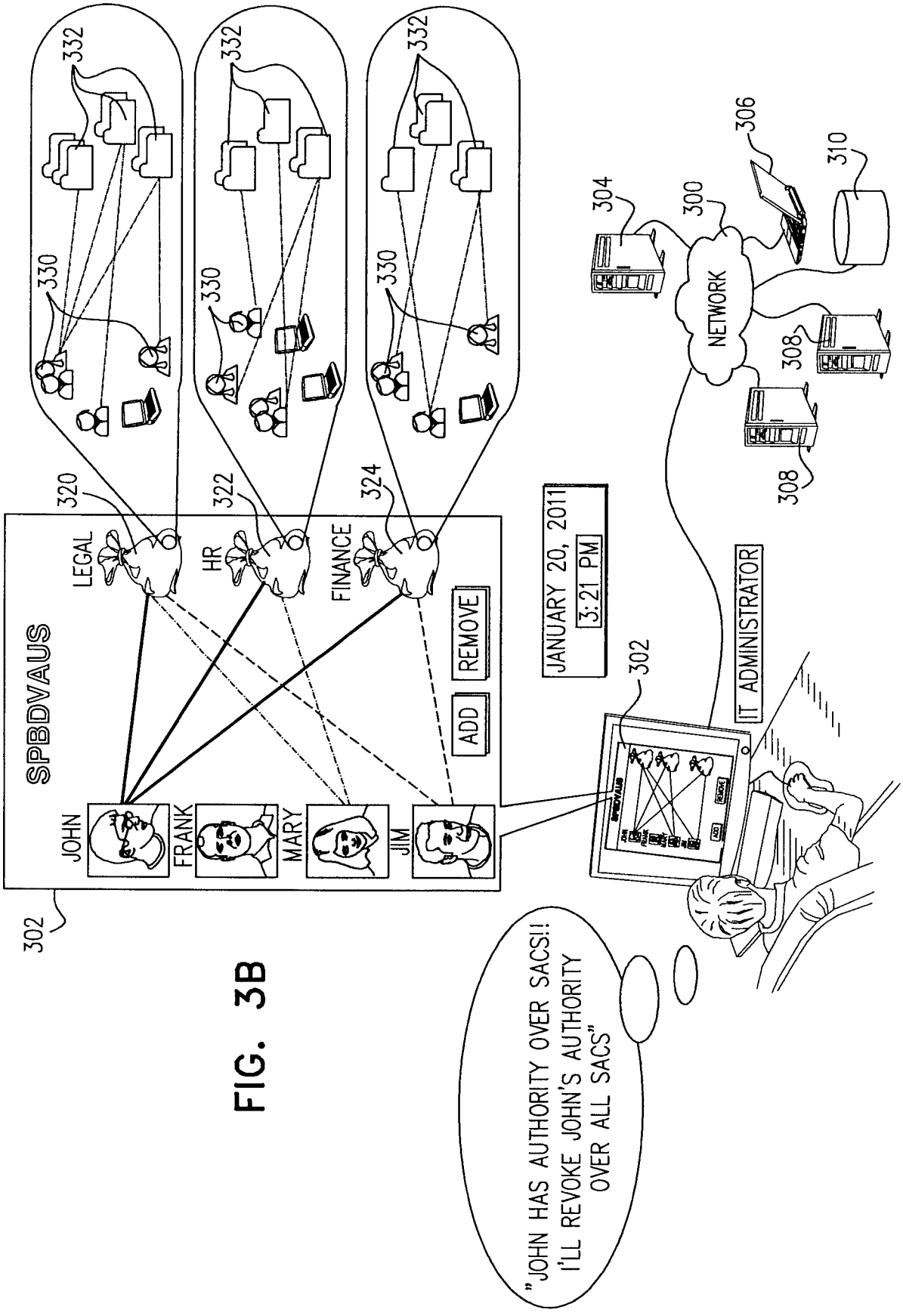

SPBDVAUS
LEGAL
HR
FINANCE
320
322
324
330
332
JOHN
FRANK
MARY
JIM
ADD
REMOVE
302
JANUARY 20, 2011
3:21 PM
IT ADMINISTRATOR
NETWORK
300
304
306
308
310
"JOHN HAS AUTHORITY OVER SACS!!
I'LL REVOKE JOHN'S AUTHORITY
OVER ALL SACS"

FIG. 3B

FIG. 3C

USER ACTIONS
USER
ACTION
JOHN
GRANTED ACCESS PERMISSIONS TO LEGAL FOLDER TO SUSAN
GRANTED ACCESS PERMISSIONS TO HR FOLDER TO JERRY
GRANTED ACCESS PERMISSIONS TO FINANCE FOLDER TO TIM
"NOW, LET'S SEE WHAT JOHN HAS BEEN UP TO LATELY"
JANUARY 20, 2011 3:25 PM
SAC ACTIONS
SAC
ACTION
LEGAL
JOHN GRANTED ACCESS PERMISSIONS TO A LEGAL FOLDER TO SUSAN
MARY GRANTED ACCESS PERMISSIONS TO A LEGAL FOLDER TO RON
JIM GRANTED ACCESS PERMISSIONS TO A LEGAL FOLDER TO DAVID
"WHAT OTHER ACTIONS WERE EXECUTED ON THE LEGAL SAC?"
JANUARY 20, 2011 3:25 PM
304
300
NETWORK
306
310
IT ADMINISTRATOR

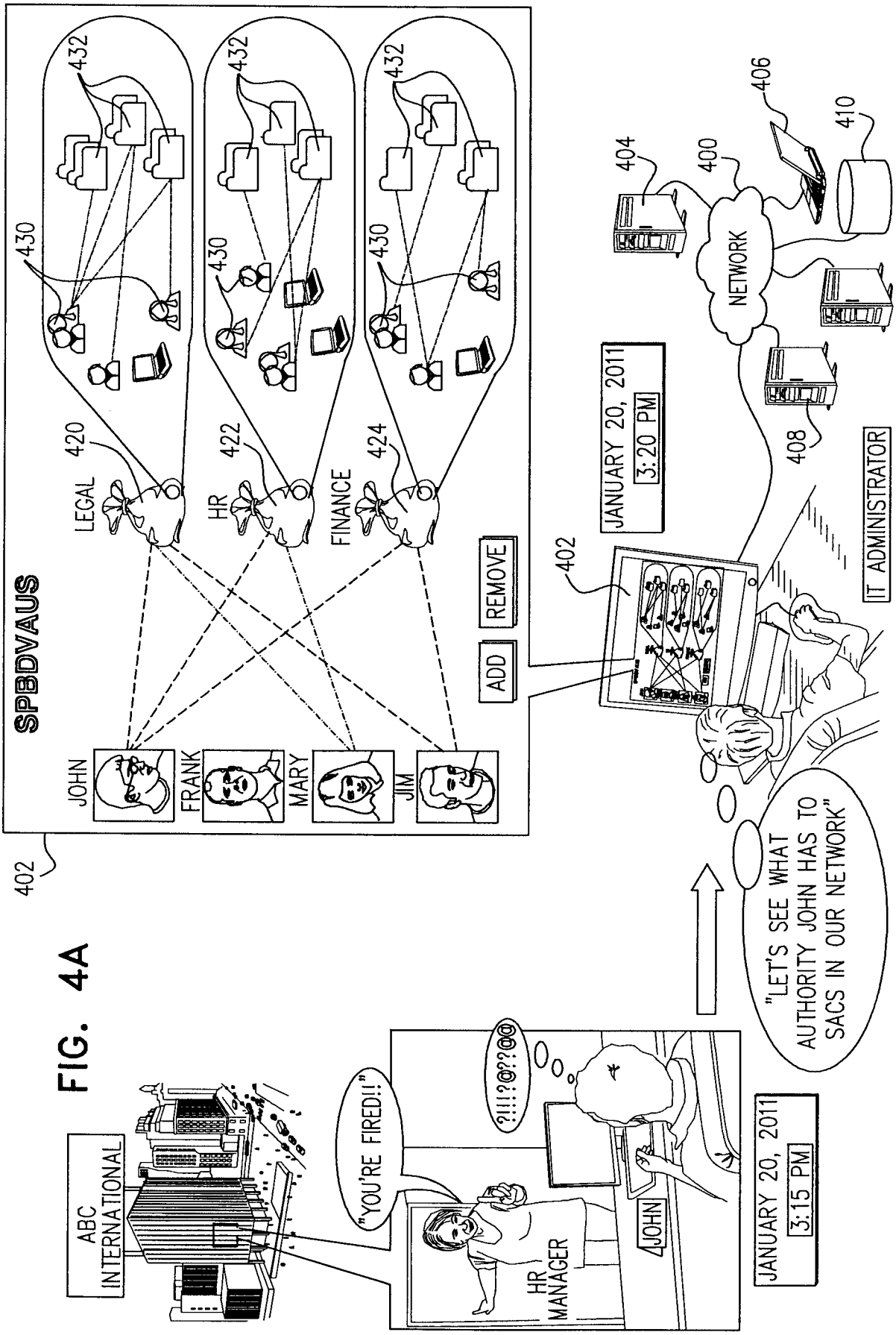

SPBDVAUS
LEGAL
HR
FINANCE
JOHN
FRANK
MARY
JIM
ADD
REMOVE
402
420
422
424
430
432
NETWORK
404
400
406
410
408
JANUARY 20, 2011
3:20 PM
IT ADMINISTRATOR
"LET'S SEE WHAT AUTHORITY JOHN HAS TO SACS IN OUR NETWORK"
ABC INTERNATIONAL
"YOU'RE FIRED!!"
?!!!?@?@@
HR MANAGER
JOHN
JANUARY 20, 2011
3:15 PM

FIG. 4A

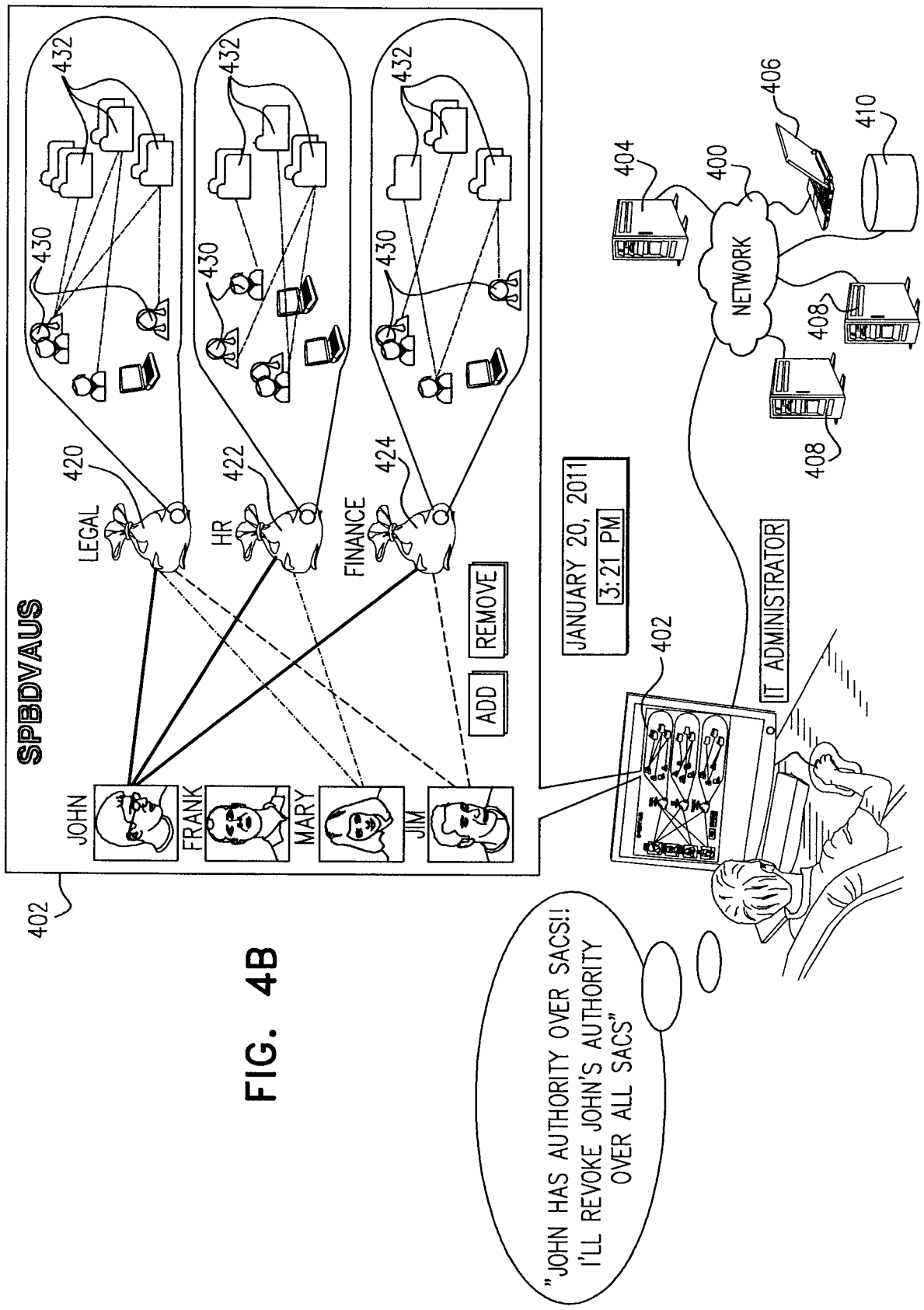

SPBDVAUS
LEGAL
HR
FINANCE
420
422
424
430
432
JOHN
FRANK
MARY
JIM
ADD
REMOVE
402
JANUARY 20, 2011
3:21 PM
IT ADMINISTRATOR
NETWORK
400
404
406
408
410
"JOHN HAS AUTHORITY OVER SACS!!
I'LL REVOKE JOHN'S AUTHORITY
OVER ALL SACS"

FIG. 4B

FIG. 4C

USER ACTIONS	
USER	ACTION
JOHN	GRANTED ACCESS PERMISSIONS TO LEGAL FOLDER TO SUSAN
	GRANTED ACCESS PERMISSIONS TO HR FOLDER TO JERRY
	GRANTED ACCESS PERMISSIONS TO FINANCE FOLDER TO TIM
⋮	⋮

SAC ACTIONS	
SAC	ACTION
LEGAL	JOHN GRANTED ACCESS PERMISSIONS TO A LEGAL FOLDER TO SUSAN
	MARY GRANTED ACCESS PERMISSIONS TO A LEGAL FOLDER TO RON
	JIM GRANTED ACCESS PERMISSIONS TO A LEGAL FOLDER TO DAVID
⋮	⋮

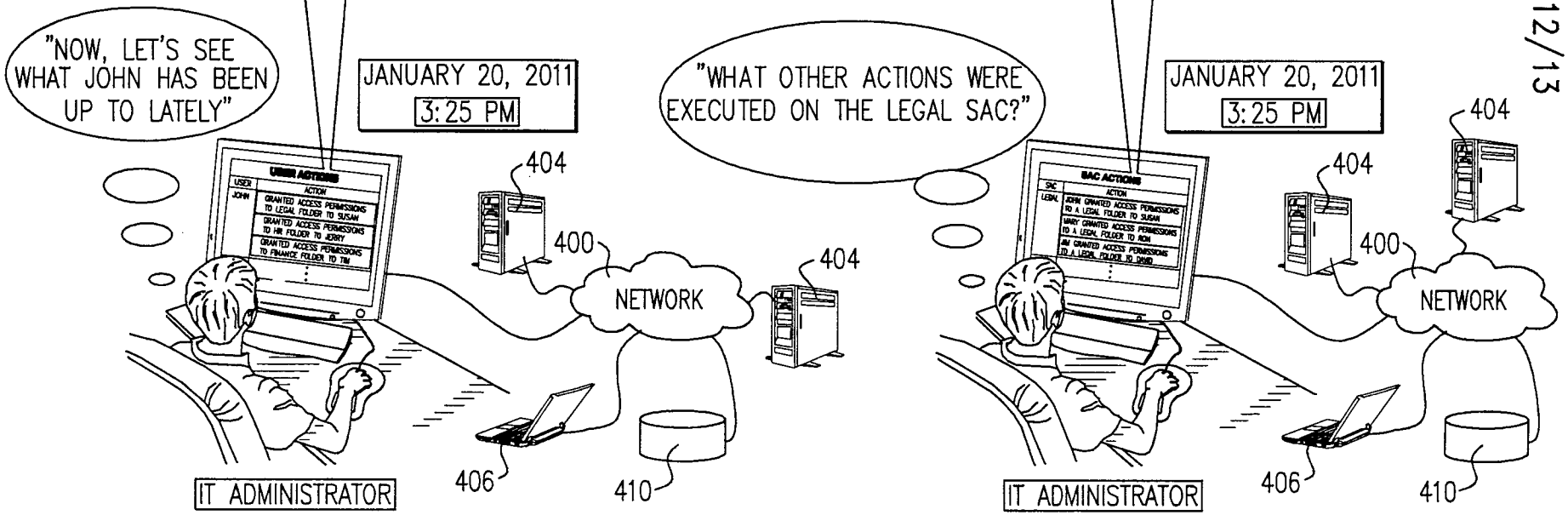
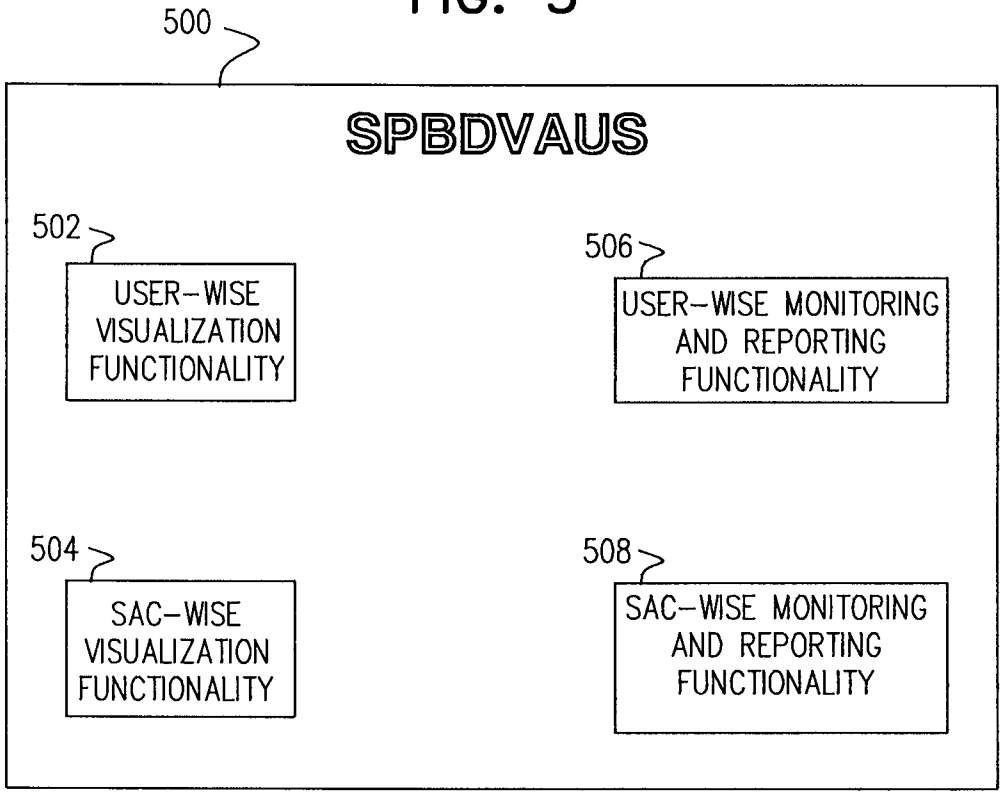


FIG. 5


500
SPBDVAUS
502
USER-WISE VISUALIZATION FUNCTIONALITY
506
USER-WISE MONITORING AND REPORTING FUNCTIONALITY
504
SAC-WISE VISUALIZATION FUNCTIONALITY
508
SAC-WISE MONITORING AND REPORTING FUNCTIONALITY

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL 11/00903

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 7/04 (2012.01)
USPC - 726/27
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)
USPC: 726/27

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 726/27-30 (text search)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PubWest (PGPB, USPT, EPAB, JPAB), Google,
Search terms used: level, directory, services, management, permission, access, database, computer, device, user, interface, gui, employee, enterprise, compan, project, task, assignment, job, authorit, authoriz, company, entity, business, network, intranet, machine

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7,305,562 B1 (Bianco et al.) 04 December 2007 (04.12.2007), Fig. 14, col. 3, ln. 32-38, col. 10, ln. 48-51, col. 18, ln. 35-50, col. 19, ln. 8-65, col. 21, ln. 13-66, col. 23, ln. 1-19, col. 27, ln. 57-64, col. 28, ln. 5-16, col. 58, ln. 45-48	1-24
Y	US 7,849,496 B2 (Ahern et al.) 07 December 2010 (07.12.2010), entire document	1-24
Y	US 2003/0074580 A1 (Knouse et al.) 17 April 2003 (17.04.2003), entire document	1-24

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

* 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 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
04 April 2012 (04.04.2012)	13 APR 2012
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)