US00RE41546E

(19) **United States**

(12) **Reissued Patent**

Vainstein

(10) **Patent Number: US RE41,546 E**

(45) **Date of Reissued Patent: Aug. 17, 2010**

(54) **METHOD AND SYSTEM FOR MANAGING SECURITY TIERS**

(76) Inventor: **Klimenty Vainstein**, 239 Shipley St. #101, San Francisco, CA (US) 94107

(21) Appl. No.: **11/797,367**

(22) Filed: **May 2, 2007**

Related U.S. Patent Documents

Reissue of:

(64) Patent No.: **6,889,210**
Issued: **May 3, 2005**
Appl. No.: **10/445,657**
Filed: **May 27, 2003**

U.S. Applications:

(63) Continuation-in-part of application No. 10/076,254, filed on Feb. 12, 2002, now Pat. No. 7,260,555.

(60) Provisional application No. 60/339,634, filed on Dec. 12, 2001.

(51) **Int. Cl.**
G06F 21/00 (2006.01)

(52) **U.S. Cl.** **705/57**; 705/50; 705/51; 705/52; 705/58; 705/64; 705/71; 705/75; 380/200; 380/201; 380/202; 380/228; 713/166; 713/200; 713/201; 713/202

(58) **Field of Classification Search** 705/57, 705/50, 51, 52, 58, 64, 71; 380/200, 201, 380/202, 228; 713/166, 200, 201, 202
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,203,166	A	5/1980	Ehrsam et al.
4,734,568	A	3/1988	Watanabe
4,757,533	A	7/1988	Allen et al.
4,796,220	A	1/1989	Wolfe
4,799,258	A	1/1989	Davies
4,827,508	A	5/1989	Shear
4,888,800	A	12/1989	Marshall et al.
4,972,472	A	11/1990	Brown et al.
5,032,979	A	7/1991	Hecht et al.
5,052,040	A	9/1991	Preston et al.
5,058,164	A	10/1991	Elmer et al.
5,144,660	A	9/1992	Rose
5,204,897	A	4/1993	Wyman
5,220,657	A	6/1993	Bly et al.

(Continued)

FOREIGN PATENT DOCUMENTS

EP	0 647 253	A1	9/1995
EP	0 672 991	A2	9/1995

(Continued)

OTHER PUBLICATIONS

Search Report, completion date Apr. 14, 2005, for European Patent Application No. EP 02 25 8533, 2 pages.

(Continued)

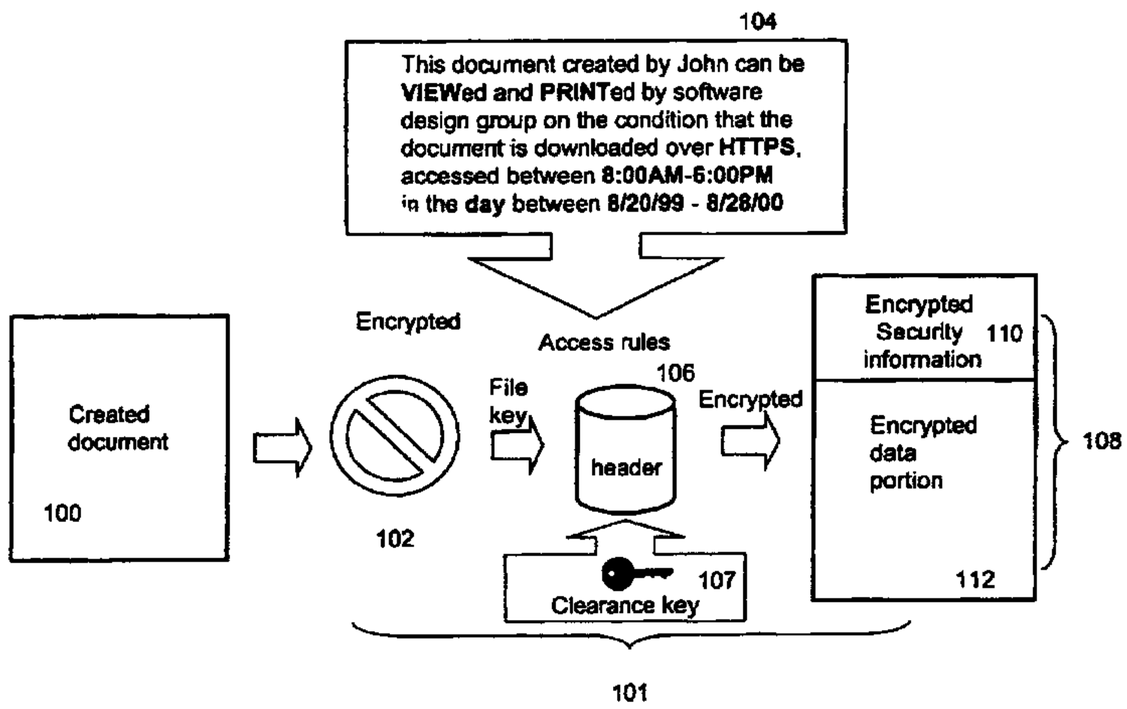
Primary Examiner—Pierre E Elisca

(74) *Attorney, Agent, or Firm*—Sterne, Kessler, Goldstein & Fox PLLC

(57) **ABSTRACT**

Techniques for reorganizing security levels without implicating accessibility to secured files classified in accordance to one of the security levels are disclosed. In a case of adding a new security level, the controllability or restrictiveness of the new security level is determined with respect to the most restrictive security level or the least security level in a set of existing security levels. A set of proper security parameters are then generated for the new security level and subsequently the existing security levels are reorganized to accommodate the new security level. In a case of removing a security level from the existing security levels, the security parameters for the security level to be deleted are either folded up or down to an immediate next security level, depending on implementation. As a result, the security parameters for the immediate next security level are updated to include those for the security level to be deleted such that the secured files classified at the security level to be deleted can still be accessed by those with proper clearance levels.

35 Claims, 12 Drawing Sheets



U.S. PATENT DOCUMENTS

5,235,641	A	8/1993	Nozawa et al.
5,247,575	A	9/1993	Sprague et al.
5,276,735	A	1/1994	Boebert et al.
5,301,247	A	4/1994	Rasmussen et al.
5,319,705	A	6/1994	Halter et al.
5,369,702	A	11/1994	Shanton
5,375,169	A	12/1994	Seheidt et al.
5,404,404	A	4/1995	Novorita
5,406,628	A	4/1995	Beller et al.
5,414,852	A	5/1995	Kramer et al.
5,495,533	A	2/1996	Linehan et al.
5,499,297	A	3/1996	Boebert
5,502,766	A	3/1996	Boebert et al.
5,535,375	A	7/1996	Eshel et al.
5,557,765	A	9/1996	Lipner et al.
5,570,108	A	10/1996	McLaughlin et al.
5,584,023	A	12/1996	Hsu
5,600,722	A	2/1997	Yamaguchi et al.
5,606,663	A	2/1997	Kadooka
5,655,119	A	8/1997	Davy
5,661,806	A	8/1997	Nevoux et al.
5,671,412	A	9/1997	Christiano
5,673,316	A	9/1997	Auerbach et al.
5,677,953	A	10/1997	Dolphin
5,680,452	A	10/1997	Shanton
5,684,987	A	11/1997	Mamiya et al.
5,689,718	A	11/1997	Sakurai et al.
5,699,428	A	12/1997	McDonnal et al.
5,708,709	A	1/1998	Rose
5,715,403	A	2/1998	Stefik
5,717,755	A	2/1998	Shanton
5,720,033	A	2/1998	Deo
5,729,734	A	3/1998	Parker et al.
5,732,265	A	3/1998	Dewitt et al.
5,745,573	A	4/1998	Lipner et al.
5,748,736	A	5/1998	Mittra
5,751,287	A	5/1998	Hahn et al.
5,757,920	A	5/1998	Misra et al.
5,765,152	A	6/1998	Erickson
5,778,065	A	7/1998	Hauser et al.
5,787,169	A	7/1998	Eldridge et al.
5,787,173	A	7/1998	Seheidt et al.
5,787,175	A	7/1998	Carter
5,790,789	A	8/1998	Suarez
5,790,790	A	8/1998	Smith et al.
5,813,009	A	9/1998	Johnson et al.
5,821,933	A	10/1998	Keller et al.
5,825,876	A	10/1998	Peterson
5,835,592	A	11/1998	Chang et al.
5,835,601	A	11/1998	Shimbo et al.
5,857,189	A	1/1999	Riddle
5,862,325	A	1/1999	Reed et al.
5,870,468	A	2/1999	Harrison
5,870,477	A	2/1999	Sasaki et al.
5,881,287	A	3/1999	Mast
5,892,900	A	4/1999	Ginter et al.
5,893,084	A	4/1999	Morgan et al.
5,898,781	A	4/1999	Shanton
5,922,073	A	7/1999	Shimada
5,923,754	A	7/1999	Angelo et al.
5,933,498	A	8/1999	Schnek et al.
5,944,794	A	8/1999	Okamoto et al.
5,953,419	A	9/1999	Lohstroh et al.
5,968,177	A	10/1999	Batten-Carew et al.
5,970,502	A	10/1999	Salkewicz et al.
5,987,440	A	11/1999	O'Neil et al.
5,991,879	A	11/1999	Still
5,999,907	A	12/1999	Donner
6,014,730	A	1/2000	Ohtsu
6,023,506	A	2/2000	Ote et al.
6,032,216	A	2/2000	Schmuck et al.
6,038,322	A	3/2000	Harkins
6,044,155	A	3/2000	Thomlinson et al.
6,055,314	A	4/2000	Spies et al.
6,058,424	A	5/2000	Dixon et al.
6,061,790	A	5/2000	Bodnar
6,069,957	A	5/2000	Richards
6,085,323	A	7/2000	Shimizu et al.
6,088,717	A	7/2000	Reed et al.
6,088,805	A	7/2000	Davis et al.
6,098,056	A	8/2000	Rusnak et al.
6,101,507	A	8/2000	Cane et al.
6,105,131	A	8/2000	Carroll
6,122,630	A	9/2000	Strickler et al.
6,134,327	A	10/2000	Van Oorschot
6,134,658	A	10/2000	Multerer et al.
6,134,660	A	10/2000	Boneh et al.
6,134,664	A	10/2000	Walker
6,141,754	A	10/2000	Choy
6,145,084	A	11/2000	Zuili
6,158,010	A	12/2000	Moriconi et al.
6,161,139	A	12/2000	Win et al.
6,182,142	B1	1/2001	Win et al.
6,185,684	B1	2/2001	Pravetz et al.
6,192,408	B1	2/2001	Vahalia et al.
6,205,549	B1	3/2001	Pravetz et al.
6,212,561	B1	4/2001	Sitaraman et al.
6,223,285	B1	4/2001	Komuro et al.
6,226,618	B1	5/2001	Downs et al.
6,226,745	B1	5/2001	Wiederhold et al.
6,240,188	B1	5/2001	Dondeti et al.
6,249,873	B1	6/2001	Richard et al.
6,253,193	B1	6/2001	Ginter et al.
6,260,040	B1	7/2001	Kauffman et al.
6,260,141	B1	7/2001	Park
6,263,348	B1	7/2001	Kathrow et al.
6,272,631	B1	8/2001	Thomlinson et al.
6,272,632	B1	8/2001	Carmen et al.
6,282,649	B1	8/2001	Lambert et al.
6,289,450	B1	9/2001	Pensak et al.
6,292,895	B1	9/2001	Baltzley
6,292,899	B1	9/2001	McBride
6,295,361	B1	9/2001	Kadansky et al.
6,301,614	B1	10/2001	Najork et al.
6,308,256	B1	10/2001	Folmsbee
6,308,273	B1	10/2001	Goertzel et al.
6,314,409	B2	11/2001	Schnek et al.
6,317,777	B1	11/2001	Skarbo et al.
6,332,025	B2	12/2001	Takahashi et al.
6,336,114	B1	1/2002	Garrison
6,339,423	B1	1/2002	Sampson et al.
6,339,825	B2	1/2002	Pensak et al.
6,341,164	B1	1/2002	Dilkie et al.
6,343,316	B1	1/2002	Sakata
6,347,374	B1	2/2002	Drake et al.
6,349,337	B1	2/2002	Parsons et al.
6,351,813	B1	2/2002	Mooney et al.
6,356,903	B1	3/2002	Baxter et al.
6,356,941	B1	3/2002	Cohen
6,357,010	B1	3/2002	Viets et al.
6,363,480	B1	3/2002	Perlman
6,370,249	B1	4/2002	Van Oorschot
6,381,698	B1	4/2002	Devanbu et al.
6,389,433	B1	5/2002	Bolosky et al.
6,389,538	B1	5/2002	Gruse et al.
6,393,420	B1	5/2002	Peters
6,405,315	B1	6/2002	Burns et al.
6,421,714	B1	7/2002	Rai et al.
6,442,688	B1	8/2002	Moses et al.
6,442,695	B1	8/2002	Dutcher et al.
6,446,090	B1	9/2002	Hart

6,449,721	B1	9/2002	Pensak et al.
6,453,353	B1	9/2002	Win et al.
6,466,932	B1	10/2002	Dennis et al.
6,477,544	B1	11/2002	Bolosky et al.
6,490,680	B1	12/2002	Scheidt et al.
6,505,300	B2	1/2003	Chan et al.
6,510,349	B1	1/2003	Schnek et al.
6,519,700	B1	2/2003	Ram et al.
6,529,956	B1	3/2003	Smith et al.
6,530,020	B1	3/2003	Aoki
6,530,024	B1	3/2003	Proctor
6,542,608	B2	4/2003	Scheidt et al.
6,549,623	B1	4/2003	Scheidt et al.
6,550,011	B1	4/2003	Sims
6,557,039	B1	4/2003	Leong et al.
6,567,914	B1	5/2003	Just et al.
6,571,291	B1	5/2003	Chow
6,584,466	B1	6/2003	Serbinis et al.
6,587,946	B1	7/2003	Jakobsson
6,588,673	B1	7/2003	Chan et al.
6,594,662	B1	7/2003	Sieffert et al.
6,598,161	B1	7/2003	Kluttz et al.
6,603,857	B1	8/2003	Batten-Carew et al.
6,608,636	B1	8/2003	Roseman
6,611,599	B2	8/2003	Natarajan
6,611,846	B1	8/2003	Stoodley
6,615,349	B1	9/2003	Hair
6,615,350	B1	9/2003	Schell et al.
6,625,650	B2	9/2003	Stelliga
6,629,243	B1	9/2003	Kleinman et al.
6,633,311	B1	10/2003	Douvikas et al.
6,640,307	B2	10/2003	Viets et al.
6,646,515	B2	11/2003	Jun et al.
6,647,388	B2	11/2003	Numao et al.
6,678,835	B1	1/2004	Shah et al.
6,687,822	B1	2/2004	Jakobsson
6,711,683	B1	3/2004	Laczko et al.
6,718,361	B1	4/2004	Basani et al.
6,735,701	B1	5/2004	Jacobson
6,738,908	B1	5/2004	Bonn et al.
6,775,779	B1	8/2004	England et al.
6,782,403	B1	8/2004	Kino et al.
6,801,999	B1	10/2004	Venkatesan et al.
6,807,534	B1	10/2004	Erickson
6,807,636	B2	10/2004	Hartman et al.
6,810,389	B1	10/2004	Meyer
6,810,479	B1	10/2004	Barlow et al.
6,816,871	B2	11/2004	Lee
6,826,698	B1	11/2004	Minkin et al.
6,834,333	B2	12/2004	Yoshino et al.
6,834,341	B1	12/2004	Bahl et al.
6,845,452	B1	1/2005	Roddy et al.
6,851,050	B2	2/2005	Singhal et al.
6,865,555	B2	3/2005	Novak
6,874,139	B2	3/2005	Krueger et al.
6,877,136	B2	4/2005	Bess et al.
6,889,210	B1	5/2005	Vainstein
6,891,953	B1	5/2005	DeMello et al.
6,892,201	B2	5/2005	Brown et al.
6,892,306	B1	5/2005	En-Seung et al.
6,907,034	B1	6/2005	Begis
6,909,708	B1	6/2005	Krishnaswamy et al.
6,915,434	B1	7/2005	Kuroda et al.
6,920,558	B2	7/2005	Sames et al.
6,931,450	B2	8/2005	Howard et al.
6,931,530	B2	8/2005	Pham et al.
6,931,597	B1	8/2005	Prakash
6,938,042	B2	8/2005	Aboulhosn et al.
6,941,355	B1	9/2005	Donaghey et al.
6,941,456	B2	9/2005	Wilson
6,941,472	B2	9/2005	Moriconi et al.
6,944,183	B1	9/2005	Iyer et al.
6,947,556	B1	9/2005	Matyas, Jr. et al.
6,950,818	B2	9/2005	Dennis et al.
6,950,936	B2	9/2005	Subramaniam et al.
6,950,941	B1	9/2005	Lee et al.
6,950,943	B1	9/2005	Bacha et al.
6,952,780	B2	10/2005	Olsen et al.
6,957,261	B2	10/2005	Lortz
6,959,308	B2	10/2005	Gramsamer et al.
6,961,849	B1	11/2005	Davis et al.
6,968,060	B1	11/2005	Pinkas
6,971,018	B1	11/2005	Witt et al.
6,978,376	B2	12/2005	Giroux et al.
6,978,377	B1	12/2005	Asano et al.
6,988,133	B1	1/2006	Zavalkovsky et al.
6,988,199	B2	1/2006	Toh et al.
6,993,135	B2	1/2006	Ishibashi
6,996,718	B1	2/2006	Henry et al.
7,003,117	B2	2/2006	Kacker et al.
7,003,560	B1	2/2006	Mullen et al.
7,003,661	B2	2/2006	Beattie et al.
7,013,332	B2	3/2006	Friedel et al.
7,013,485	B2	3/2006	Brown et al.
7,020,645	B2	3/2006	Bisbee et al.
7,024,427	B2	4/2006	Bobbitt et al.
7,035,854	B2	4/2006	Hsiao et al.
7,035,910	B1	4/2006	Dutta et al.
7,046,807	B2	5/2006	Hirano et al.
7,051,213	B1	5/2006	Kobayashi et al.
7,058,696	B1	6/2006	Phillips et al.
7,058,978	B2	6/2006	Feuerstein et al.
7,073,063	B2	7/2006	Peinado
7,073,073	B1	7/2006	Nonaka et al.
7,076,067	B2	7/2006	Raike et al.
7,076,312	B2	7/2006	Law et al.
7,076,469	B2	7/2006	Schreiber et al.
7,076,633	B2	7/2006	Tormasov et al.
7,080,077	B2	7/2006	Ramamurthy et al.
7,095,853	B2	8/2006	Morishita
7,096,266	B2	8/2006	Lewin et al.
7,099,926	B1	8/2006	Ims et al.
7,107,269	B2	9/2006	Arlein et al.
7,107,416	B2	9/2006	Stuart et al.
7,117,322	B2	10/2006	Hochberg et al.
7,120,635	B2	10/2006	Bhide et al.
7,120,757	B2	10/2006	Tsuge
7,124,164	B1	10/2006	Chemtob
7,130,964	B2	10/2006	Ims et al.
7,131,071	B2	10/2006	Gune et al.
7,134,041	B2	11/2006	Murray et al.
7,136,903	B1	11/2006	Phillips et al.
7,145,898	B1	12/2006	Elliott
7,146,388	B2	12/2006	Stakutis et al.
7,146,498	B1	12/2006	Takechi et al.
7,159,036	B2	1/2007	Hinchliffe et al.
7,171,557	B2	1/2007	Kallahalla et al.
7,174,563	B1	2/2007	Brownlie et al.
7,177,427	B1	2/2007	Komuro et al.
7,178,033	B1	2/2007	Garcia
7,181,017	B1	2/2007	Nagel et al.
7,185,364	B2	2/2007	Knouse et al.
7,187,033	B2	3/2007	Pendharkar
7,188,181	B1	3/2007	Squier et al.
7,194,764	B2	3/2007	Martherus et al.
7,200,747	B2	4/2007	Riedel et al.
7,203,317	B2	4/2007	Kallahalla et al.
7,203,968	B2	4/2007	Asano et al.
7,219,230	B2	5/2007	Riedel et al.
7,224,795	B2	5/2007	Takada et al.
7,225,256	B2	5/2007	Villavicencio
7,227,953	B2	6/2007	Shida

7,233,948	B1	6/2007	Shamoon et al.	
7,237,002	B1	6/2007	Estrada et al.	
7,249,044	B2	7/2007	Kumar et al.	
7,260,555	B2	8/2007	Rossmann et al.	
7,265,764	B2	9/2007	Alben et al.	
7,266,684	B2	9/2007	Jancula	
7,280,658	B2	10/2007	Amini et al.	
7,287,055	B2	10/2007	Smith et al.	
7,290,148	B2	10/2007	Tozawa et al.	
7,308,702	B1	12/2007	Thomsen et al.	
7,313,824	B1	12/2007	Bala et al.	
7,319,752	B2	1/2008	Asano et al.	
7,340,600	B1	3/2008	Corella	
7,362,868	B2 *	4/2008	Madoukh et al.	380/277
7,380,120	B1	5/2008	Garcia	
7,383,586	B2	6/2008	Cross et al.	
7,386,529	B2	6/2008	Kiessig et al.	
2001/0011254	A1	8/2001	Clark	
2001/0021926	A1	9/2001	Schnek et al.	
2001/0032181	A1	10/2001	Jakstadt et al.	
2001/0034839	A1	10/2001	Karjoth et al.	
2001/0044903	A1	11/2001	Yamamoto et al.	
2001/0056550	A1	12/2001	Lee	
2002/0010679	A1	1/2002	Felsher	
2002/0016922	A1	2/2002	Richards et al.	
2002/0031230	A1	3/2002	Sweet et al.	
2002/0035624	A1	3/2002	Kim	
2002/0046350	A1	4/2002	Lordemann et al.	
2002/0050098	A1	5/2002	Chan	
2002/0056042	A1	5/2002	Van Der Kaay et al.	
2002/0062240	A1	5/2002	Morinville	
2002/0062245	A1	5/2002	Niu et al.	
2002/0069077	A1	6/2002	Brophy et al.	
2002/0069272	A1	6/2002	Kim et al.	
2002/0069363	A1	6/2002	Winburn	
2002/0073320	A1	6/2002	Rinkevich et al.	
2002/0077986	A1	6/2002	Kobata et al.	
2002/0077988	A1	6/2002	Sasaki et al.	
2002/0087479	A1	7/2002	Malcolm	
2002/0099947	A1	7/2002	Evans	
2002/0124180	A1	9/2002	Hagman	
2002/0129235	A1	9/2002	Okamoto et al.	
2002/0133699	A1	9/2002	Pueschel	
2002/0138762	A1	9/2002	Horne	
2002/0143710	A1	10/2002	Liu	
2002/0143906	A1	10/2002	Tormasov et al.	
2002/0156726	A1	10/2002	Kleckner et al.	
2002/0157016	A1	10/2002	Russell et al.	
2002/0169963	A1	11/2002	Seder et al.	
2002/0169965	A1	11/2002	Hale et al.	
2002/0172367	A1	11/2002	Mulder et al.	
2002/0174109	A1	11/2002	Chandy et al.	
2002/0176572	A1	11/2002	Ananth	
2002/0178271	A1	11/2002	Graham et al.	
2002/0194484	A1	12/2002	Bolosky et al.	
2002/0198798	A1	12/2002	Ludwig et al.	
2003/0009685	A1	1/2003	Choo et al.	
2003/0014391	A1	1/2003	Evans et al.	
2003/0023559	A1	1/2003	Choi et al.	
2003/0028610	A1	2/2003	Pearson	
2003/0033528	A1	2/2003	Ozog et al.	
2003/0037133	A1	2/2003	Owens	
2003/0037237	A1	2/2003	Abgrall et al.	
2003/0037253	A1	2/2003	Blank et al.	
2003/0046238	A1	3/2003	Nonaka et al.	
2003/0051039	A1	3/2003	Brown et al.	
2003/0056139	A1	3/2003	Murray et al.	
2003/0074580	A1	4/2003	Knouse et al.	
2003/0078959	A1	4/2003	Yeung et al.	
2003/0079175	A1	4/2003	Limantsev	
2003/0081784	A1	5/2003	Kallahalla et al.	
2003/0081787	A1	5/2003	Kallahalla et al.	
2003/0088517	A1	5/2003	Medoff	
2003/0088783	A1	5/2003	DiPierro	
2003/0101072	A1	5/2003	Dick et al.	
2003/0110169	A1	6/2003	Zuili	
2003/0110266	A1	6/2003	Rollins et al.	
2003/0110397	A1	6/2003	Supramaniam	
2003/0115146	A1	6/2003	Lee et al.	
2003/0115570	A1	6/2003	Bisceglia	
2003/0120601	A1	6/2003	Ouye	
2003/0120684	A1	6/2003	Zuili et al.	
2003/0126434	A1	7/2003	Lim et al.	
2003/0154381	A1	8/2003	Ouye	
2003/0159066	A1	8/2003	Staw et al.	
2003/0172280	A1	9/2003	Scheidt et al.	
2003/0177070	A1	9/2003	Viswanth et al.	
2003/0177378	A1	9/2003	Wittkotter	
2003/0182579	A1	9/2003	Leporini et al.	
2003/0196096	A1	10/2003	Sutton	
2003/0197729	A1	10/2003	Denoue et al.	
2003/0200202	A1	10/2003	Hsiano et al.	
2003/0217264	A1	11/2003	Martin et al.	
2003/0217281	A1	11/2003	Ryan	
2003/0217333	A1	11/2003	Smith et al.	
2003/0226013	A1	12/2003	Dutertre	
2003/0233650	A1	12/2003	Zaner et al.	
2004/0022390	A1	2/2004	McDonald et al.	
2004/0025037	A1	2/2004	Hair	
2004/0039781	A1	2/2004	LaVallee et al.	
2004/0064710	A1	4/2004	Vainstein	
2004/0068524	A1	4/2004	Aboulhosn et al.	
2004/0068664	A1	4/2004	Nachenberg et al.	
2004/0073660	A1	4/2004	Toomey	
2004/0073718	A1	4/2004	Johannessen et al.	
2004/0088548	A1	5/2004	Smetters et al.	
2004/0098580	A1	5/2004	DeTreville	
2004/0103202	A1	5/2004	Hildenbrand et al.	
2004/0103280	A1	5/2004	Balfanz et al.	
2004/0133544	A1	7/2004	Kiessig et al.	
2004/0158586	A1	8/2004	Tsai	
2004/0193602	A1	9/2004	Liu et al.	
2004/0193905	A1	9/2004	Lirov et al.	
2004/0193912	A1	9/2004	Li et al.	
2004/0199514	A1	10/2004	Rosenblatt et al.	
2004/0215956	A1	10/2004	Venkatachary et al.	
2004/0215962	A1	10/2004	Douceur et al.	
2004/0243853	A1	12/2004	Swander et al.	
2005/0021467	A1	1/2005	Franzdonk	
2005/0021629	A1	1/2005	Cannata et al.	
2005/0028006	A1	2/2005	Leser et al.	
2005/0039034	A1	2/2005	Doyle et al.	
2005/0071275	A1	3/2005	Vainstein et al.	
2005/0071657	A1	3/2005	Ryan	
2005/0071658	A1	3/2005	Nath et al.	
2005/0081029	A1	4/2005	Thornton et al.	
2005/0086531	A1	4/2005	Kenrich	
2005/0091484	A1	4/2005	Thornton et al.	
2005/0120199	A1	6/2005	Carter	
2005/0138371	A1	6/2005	Supramaniam	
2005/0138383	A1	6/2005	Vainstein	
2005/0177716	A1	8/2005	Ginter et al.	
2005/0177858	A1	8/2005	Ueda	
2005/0198326	A1	9/2005	Schlimmer et al.	
2005/0223242	A1	10/2005	Nath	
2005/0223414	A1	10/2005	Kenrich et al.	
2005/0235154	A1	10/2005	Serret-Avila	
2005/0256909	A1	11/2005	Aboulhosn et al.	
2005/0273600	A1	12/2005	Seeman	
2005/0283610	A1	12/2005	Serret-Avila et al.	
2005/0288961	A1	12/2005	Tabrizi	
2006/0005021	A1	1/2006	Torrubia-Saez	

2006/0075465	A1	4/2006	Ramanathan et al.
2006/0093150	A1	5/2006	Reddy et al.
2006/0168147	A1	7/2006	Inoue et al.
2006/0230437	A1	10/2006	Boyer et al.
2007/0006214	A1	1/2007	Dubal et al.
2007/0067837	A1	3/2007	Schuster

FOREIGN PATENT DOCUMENTS

EP	0 809 170	A1		11/1997
EP	0 913 966	A2		5/1999
EP	0 913 967	A2		5/1999
EP	0 950 941	A3		10/1999
EP	0 950 941	A2		10/1999
EP	1 107504	A2		6/2001
EP	1 107 504	B1		6/2001
EP	1 130 492	A2		9/2001
EP	1 154 348	A2		11/2001
EP	1324565	A1		7/2003
GB	2 328 047	A		2/1999
JP	2001-036517			2/2001
JP	02001036517	A		2/2001
JP	2006244044	A	*	9/2006
WO	WO 96/41288	A1		12/1996
WO	WO 01/61438	A2		8/2001
WO	WO 01/63387	A2		8/2001
WO	WO 01/63387	A3		8/2001
WO	WO 01/77783	A2		10/2001
WO	WO 01/78285	A1		10/2001
WO	WO 01/84271	A2		11/2001

OTHER PUBLICATIONS

Search Report, completion date Mar. 16, 2005, for European Patent Application No. EP 02 25 8534, 2 pages.

Search Report, completion date Mar. 2, 2005, for European Patent Application No. EP 02 25 8535, 2 pages.

Search Report, completion date Mar. 3, 2005, for European Patent Application No. EP 02 25 8537, 2 pages.

Search Report, completion date May 12, 2005, for European Patent Application No. EP 02 25 8539, 2 pages.

Search Report, completion date Jul. 6, 2005, for European Patent Application No. EP 02 25 8529, 4 pages.

Search Report, completion date Oct. 8, 2003, for European Patent Application No. EP 02 25 8536, 2 pages.

Search Report, completion date May 8, 2003, for European Patent Application No. EP 02 25 8540, 2 pages.

U.S. Appl. No. 10/259,075, entitled "Effectuating Access Policy Changes to Designated Places for Secured Files," inventor Crocker, Sep. 27, 2002, 60 pgs.

U.S. Appl. No. 10/286,575, entitled "Method and Architecture for Providing Acess to Secured Data from Non–Secured Clients," inventor Vainstein, Nov. 1, 2002, 46 pgs.

U.S. Appl. No. 10/295,363, entitled "Security System Using Indirect Key Generation from Access Rules and Methods Therefor," inventor Vainstein, Nov. 15, 2002, 70 pgs.

U.S. Appl. No. 11/889,310, entitled "Methods and Systems for Providing Access Control to Electronic Data, " inventor Rossmann, Aug. 10, 2007, 90 pgs.

Adobe Acrobat 5.0 Classroom in a Book, Adobe Press, Jun. 26, 2001, pp. 1–4.

Adobe Acrobat Security Settings, Acrobat 7.0, Nov. 15, 2004, pp. 1–4.

"Security Options". Dec. 20, 2001. DC & Co. pp. 1–2.

Microsoft Press Computer Dictionary, 1997, Microsoft Press, Third Edition, p. 426.

Search Report, completion date May 8, 2003, for European Patent Application No. EP 02 25 8530, 2 pages.

Search Report, completion date Oct. 2, 2003, for European Patent Application No. EP 02 25 8531, 2 pages.

U.S. Appl. No. 10/074,194, entitled "Methods for identifying compunds that inhibit or reduce PTP1B expressions" inventor Rondinone, Feb. 12, 2002, 69 pgs.

U.S. Appl. No. 10/074,804, entitled "Secured Data Format for Access Control," inventor Garcia, Feb. 12, 2002, 108 pgs.

U.S. Appl. No. 10/075,194, entitled "System and Method for Providing Multi–location Access Management to Secured Items," inventor Vainstein et al., Feb. 12, 2002, 110 pgs.

U.S. Appl. No. 10/074,996, entitled "Method and Apparatus for Securing Electronic Data," inventor Lee et al., Feb. 12, 2002, 111 pgs.

U.S. Appl. No. 10/074,825, entitled "Method and Apparatus for Accessing Secured Electronic Data Off–line, " inventor Lee et al., Feb. 12, 2002, 108 pgs.

U.S. Appl. No. 10/105,532, entitled "System and Method for Providing Different Levels of Key Security for Controlling Access to Secured Items," inventor Hildebrand et al., Mar. 20, 2002, 86 pgs.

U.S. Appl. No. 10/186,203, entitled "Method and System for Implementing Changes to Security Policies in a Distributed Security System," inventor Huang, Jun. 26, 2002, 65 pgs.

U.S. Appl. No. 10/201,756, entitled "Managing Secured Files in Designated Locations," inventor Alain, Jul. 22, 2002, 121 pgs.

U.S. Appl. No. 10/206,737, entitled "Method and System for Updating Keys in a Distributed Security System," inventor Hildebrand, Jul. 26, 2002, 60 pgs.

U.S. Appl. No. 10/246,079, entitled "Security System for Generating Keys from Access rules in a Decentralized Manner and Methods Therefor," inventor Hildebrand, Sep. 17, 2002, 78 pgs.

A Real–Time Push–Pull Communications Model for Distributed Real–Time and Multimedia Systems, Jan. 1999, School of Computer Sciences Carnegie Mellon University, Kanaka Juvva, Raj Rajkurmar.

U.S. Appl. No. 10/889,685, entitled "Method and Apparatus for Controlling the Speed Ranges of a Machine" inventor Thomas, Jul. 13, 2004, 18 pgs.

U.S. Appl. No. 10/028,397, entitled "Method and system for resisting use of a clipboard application," inventor Zuili, Dec. 21, 2001, 38 pgs.

U.S. Appl. No. 10/368,277, entitled "Method and apparatus for uniquely identifying files," inventor Ouye, Feb. 18, 2003, 25 pgs.

U.S. Appl. No. 10/327,320, entitled "Security system with staging capabilities" inventor Vainstein, Dec. 20, 2002, 39 pgs.

U.S. Appl. No. 10/286,524, entitled "Security system that uses indirect password–based encryption, " inventor Gutnik, Nov. 1, 2002, 38 pgs.

U.S. Appl. No. 10/242,185, entitled "Method and system for protecting encrypted files transmitted over a network " inventor Ryan, Sep. 11, 2002, 23 pgs.

U.S. Appl. No. 10/642,041, entitled "Method and system for fault–tolerant transfer of files across a network" inventor Kenrich, Aug. 15, 2003, 32 pgs.

U.S. Appl. No. 10/610,832, entitled "Method and system for enabling users of a group shared across multiple security systems to access secured files" inventor Ryan, Jun. 30, 2003, 33 pgs.

U.S. Appl. No. 10/448,806, entitled "Method and System for Using Remote Headers to Secure Electronic Files" inventor Ryan, May 30, 2003, 35 pgs.

"Windows 2000 EFS" in the Apr. 1999 issue of Windows NT magazine.

Microsoft Windows 200 server. Windows 2000 Group Policy White Paper, 2000.

Symantec. Norton Antivirus Corporate Edition Implementation Guide, 1999.

Crocker, Steven Toye, "Multi–level cryptographic transformations for securing digital assets," U.S. Appl. No. 10/404,566,, filed Mar. 31, 2003.

Crocker, Steven Toye, "Effectuating access policy changes to designated places for secured files," U.S. Appl. No. 10/259,075, filed Sep. 27, 2002.

Kenrich, Michael Frederick, "Multi–Level File Digest", U.S. Appl. No. 10/894,493, filed Jul. 19, 2004.

Kinghorn, Gary Mark, "Method and system for protecting electronic data in enterprise environment," U.S. Appl. No. 10/159,220, filed May 31, 2002.

Nath, Satyajit, "Method and system for securing digital assets using content type designations," U.S. Appl. No. 10/405,587, filed Apr. 1, 2003.

Prakash, Nalini J., "Method and apparatus for securiting/unsecuring files crawling," U.S. Appl. No. 10/325,102, filed Dec. 20, 2002.

Rossmann, Alain, "Hybrid systems for securing digital assets," U.S Appl. No. 10/325,013, filed Dec. 20, 2002.

Expiration Mechanism for Chipcards, IBM Technical Disclosure Bulletin, Oct. 1, 2001, UK.

McDaniel et al. "Antigone: A Flexible Framework for Secure Group Communication," Proceedings of the 8th USENIX Security Symposium, Aug. 23, 1999.

Stallings, William, "Cryptography and Network Security: Principles and Practice" 1999, pp. 333–337, Second Edition, Prentice Hall, Upper Saddle River, New Jersey.

"Affect," The American Hertage Dictionary of the English Language, Fourth Edition, Houghton Mifflin Company, 2002. Retrieved May 4, 2006 from http://dictionary.reference.com/search?q=affect.

"Inside Encryping file system," Part 1, from MSDN Oct. 2001, version, exact publication date is unknown but believed prior to Dec. 12, 2001.

"Inside Encryping file system," Part 2, from MSDN Oct. 2001 version, exact publication date is unknown but believed prior to Dec. 12, 2001.

"Security with Encryping File System," from MSDN Oct. 2001 version, exact publication date is unknown but believed prior to Dec. 12, 2001.

"How EFS work," from MSDN Oct. 2001 version, exact publication date is unknown but believed prior to Dec. 12, 2001.

"Encryping File System," from MSDN Oct. 2001 version, exact publication date is unknown but believed prior to Dec. 12, 2001.

"Features of EFS" from MSDN Oct. 2001 version, exact publication date is unknown but believed prior to Dec. 12, 2001.

Examination Report, completion date Jun. 18, 2008, for European Patent Application No. EP 02 258 532.7–1244, 6 pgs.

Office Action, dated May 10, 2005, for European Patent Application No. 02258532.7, 5 pgs.

Office Action, dated Dec. 5, 2006, for European Patent Application No. 02258532.7, 5 pgs.

Boneh et al., "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Advances in Cryptology—EUROCRYPT 2005, vol. 3493, Jun. 20, 2005, pp. 440–456.

Boneh et al., "IBE Secure E–Mail," Stanford University, Apr. 8, 2002.

IBM Technical Disclosure bulletin; Oct. 2001 UK; Expiration mechanism for chipcards.*

* cited by examiner

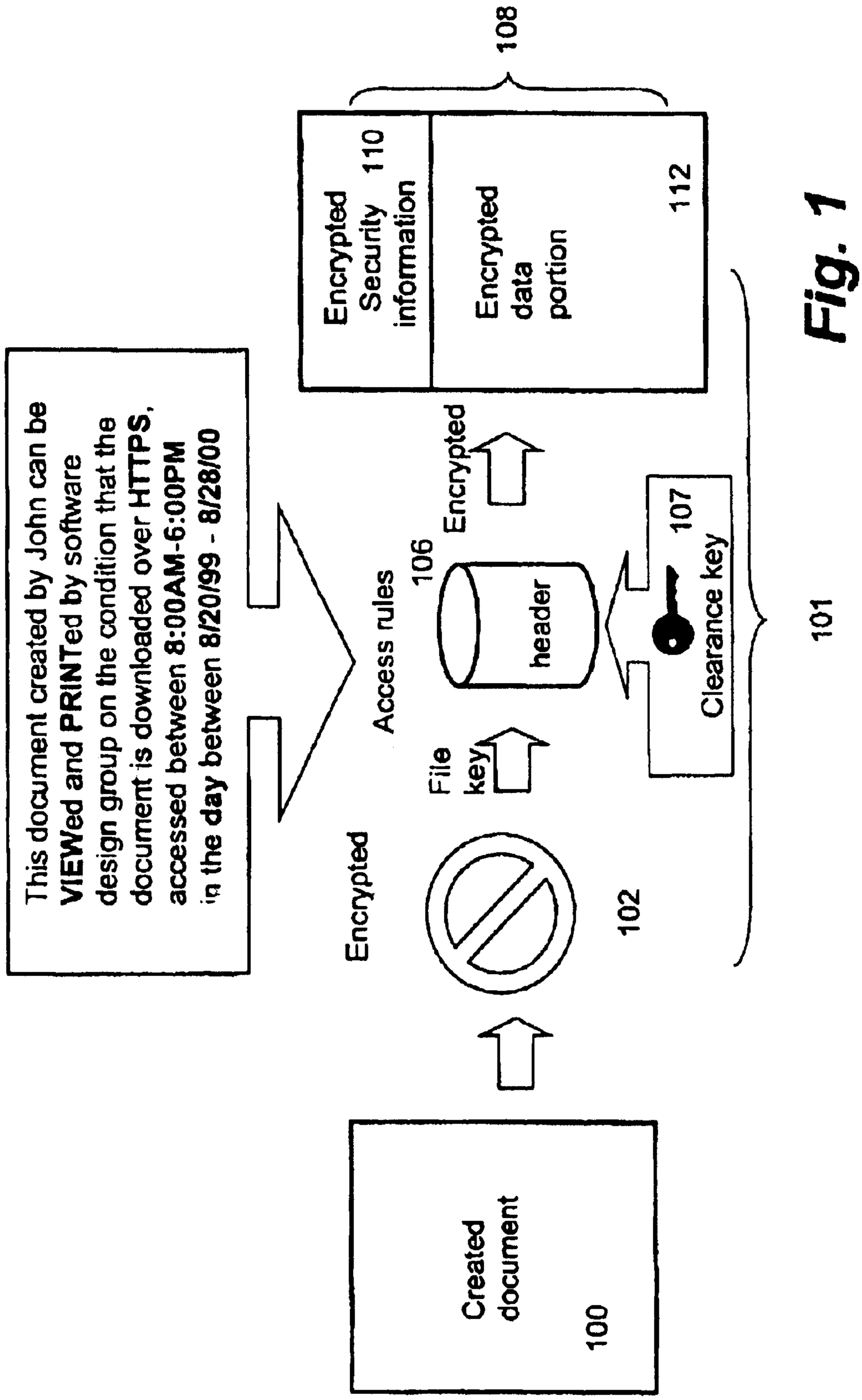

Created document
100
Encrypted
Access rules
File key
header
106
Encrypted
Clearance key
107
102
101
104
This document created by John can be VIEWed and PRINTed by software design group on the condition that the document is downloaded over HTTPS, accessed between 8:00AM-6:00PM in the day between 8/20/99 - 8/28/00
108
Encrypted Security information 110
Encrypted data portion
112

Fig. 1

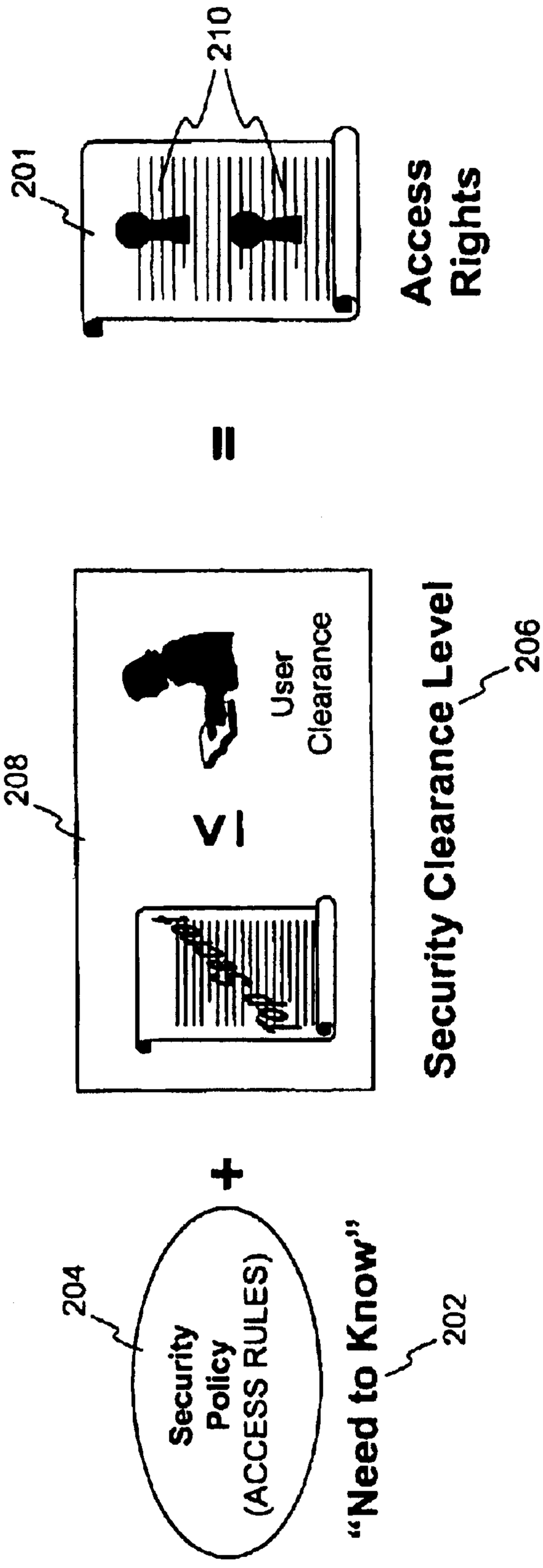

200
201
210
Access Rights
=
208
User Clearance
VI
Security Clearance Level
206
+
204
Security Policy (ACCESS RULES)
"Need to Know"
202

Fig. 2A

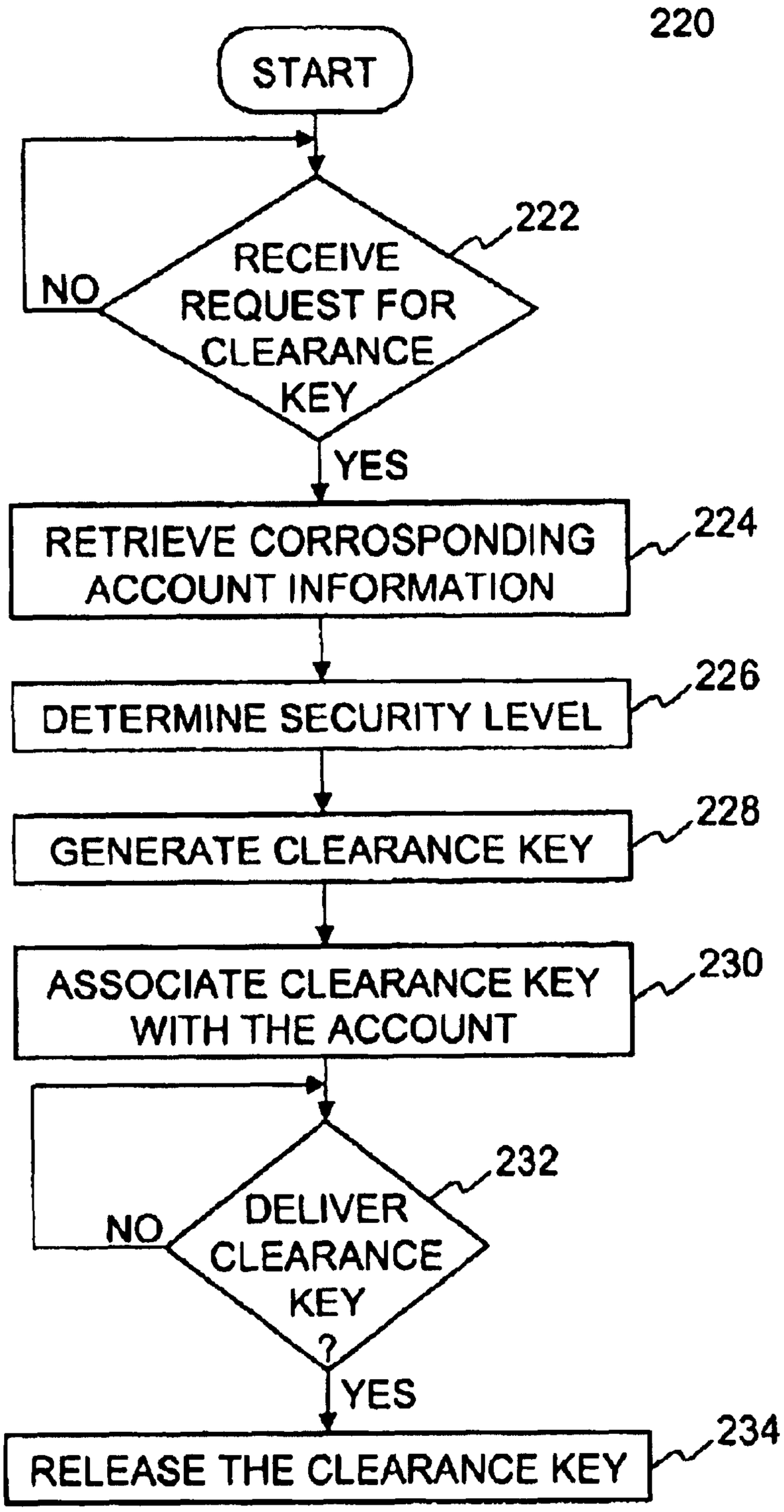

220
START
222
RECEIVE REQUEST FOR CLEARANCE KEY
NO
YES
224
RETRIEVE CORROSPONDING ACCOUNT INFORMATION
226
DETERMINE SECURITY LEVEL
228
GENERATE CLEARANCE KEY
230
ASSOCIATE CLEARANCE KEY WITH THE ACCOUNT
232
DELIVER CLEARANCE KEY ?
NO
YES
234
RELEASE THE CLEARANCE KEY

Fig. 2B

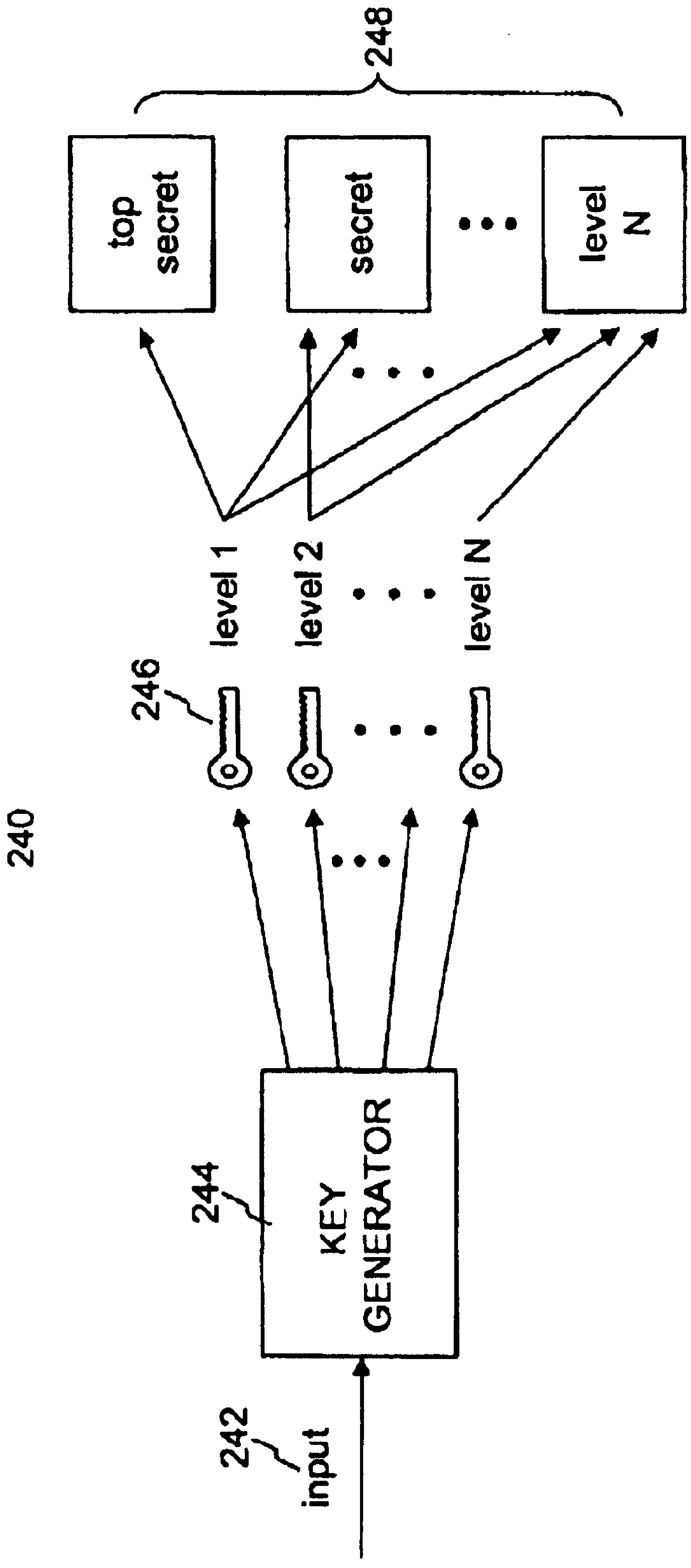
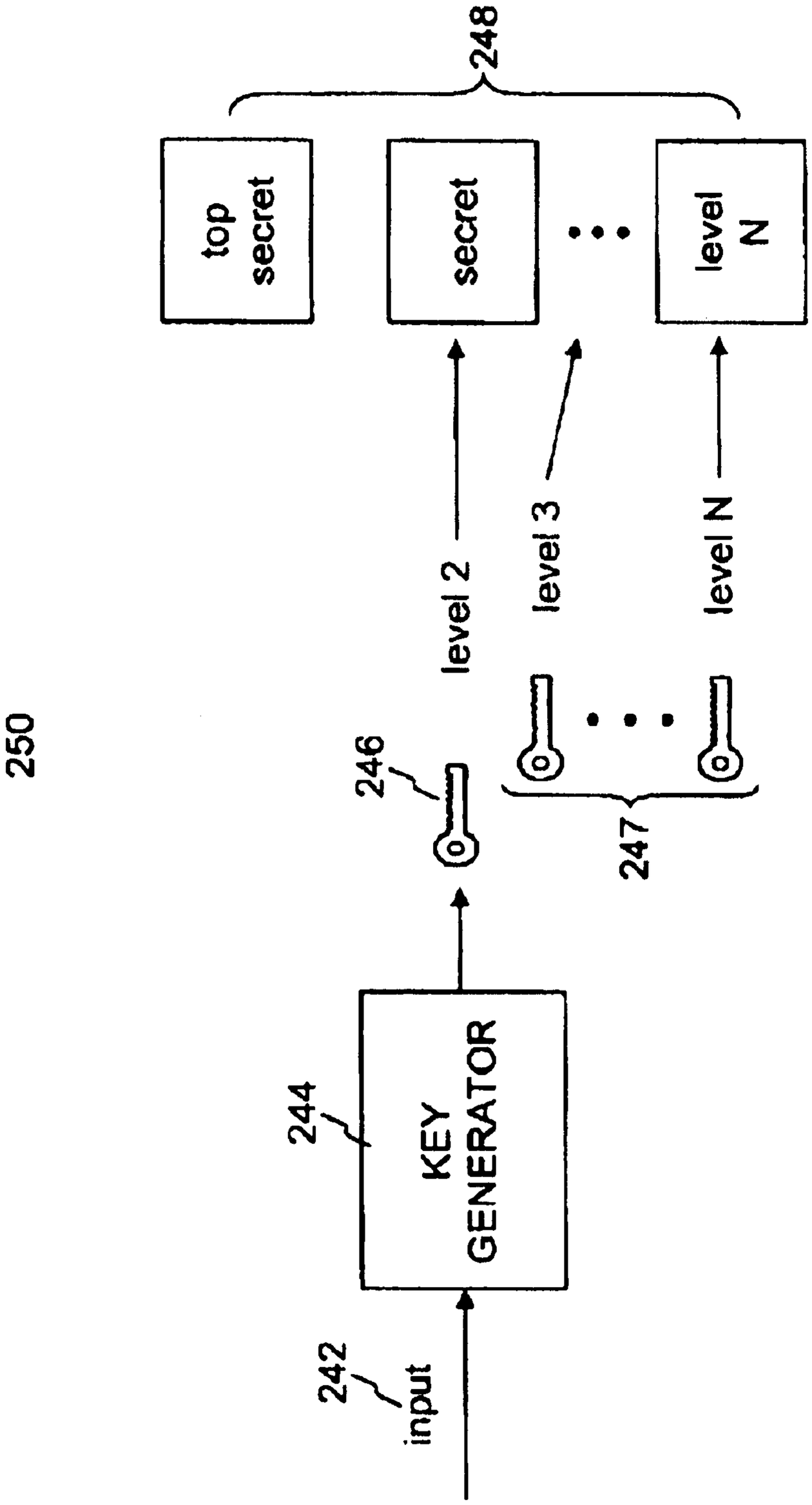

240
248
top secret
secret
level N
level 1
level 2
level N
246
244
KEY GENERATOR
242
input

Fig. 2C

Fig. 2D


248
top secret
secret
level N
level 2
level 3
level N
246
247
250
244
KEY GENERATOR
242
input

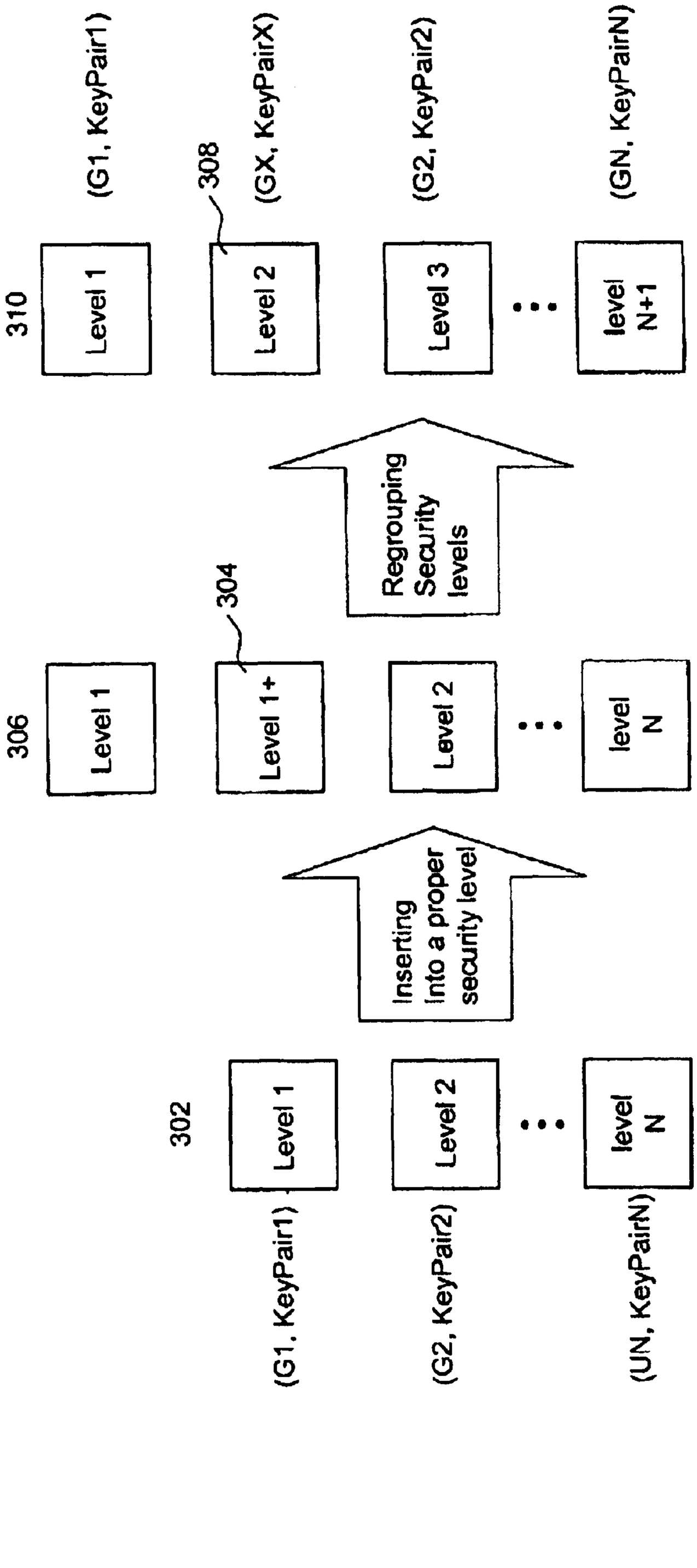

310
Level 1
(G1, KeyPair1)
308
Level 2
(GX, KeyPairX)
Level 3
(G2, KeyPair2)
level N+1
(GN, KeyPairN)
306
Level 1
304
Level 1+
Level 2
level N
Regrouping Security levels
Inserting into a proper security level
302
Level 1
(G1, KeyPair1)
Level 2
(G2, KeyPair2)
level N
(UN, KeyPairN)

FIG. 3A

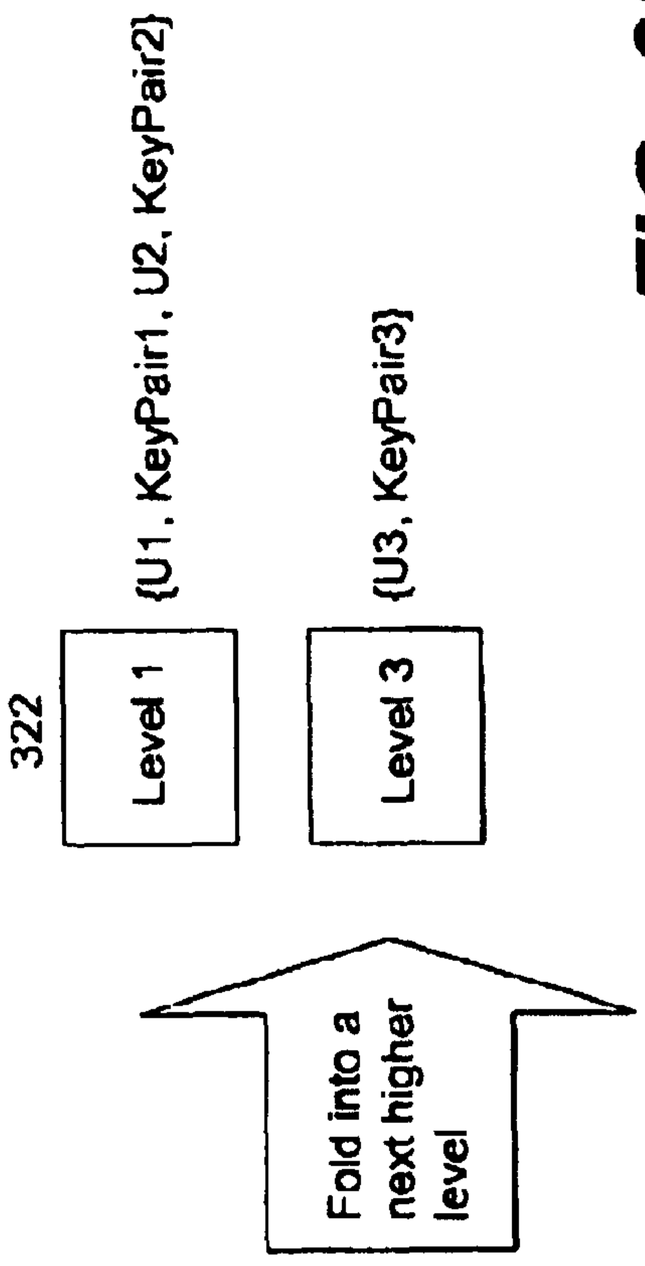

322
Level 1
{U1, KeyPair1, U2, KeyPair2}
Level 3
{U3, KeyPair3}
Fold into a next higher level

FIG. 3B

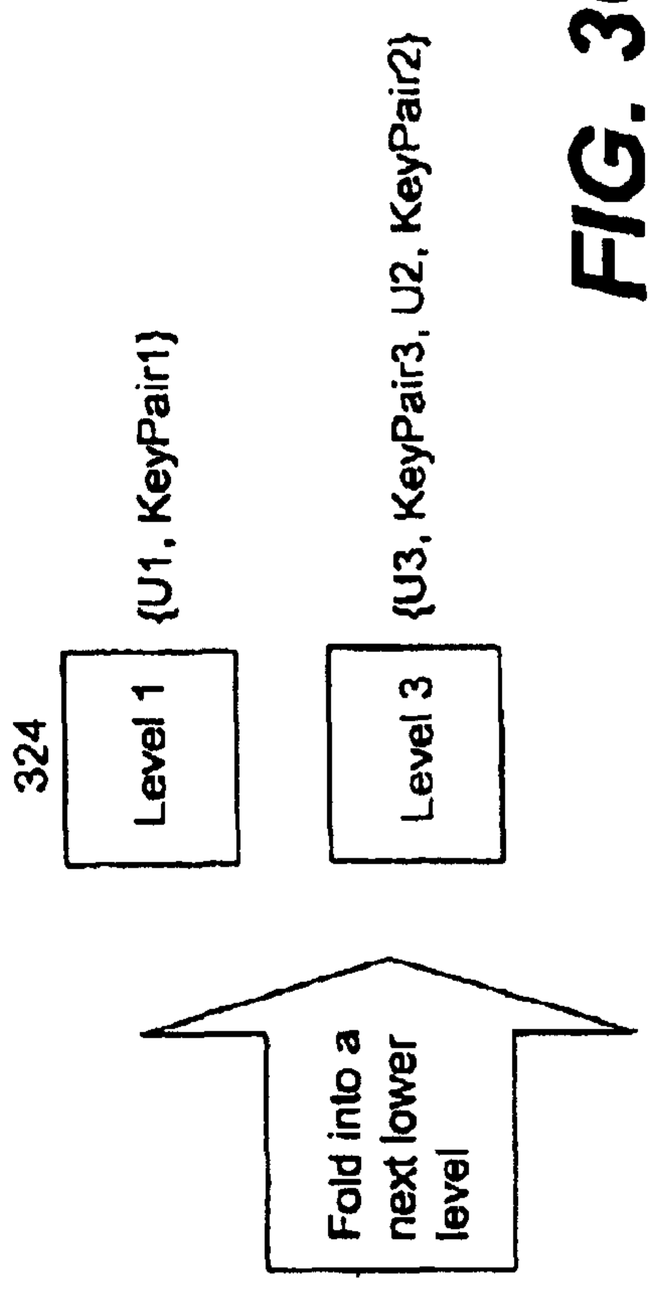
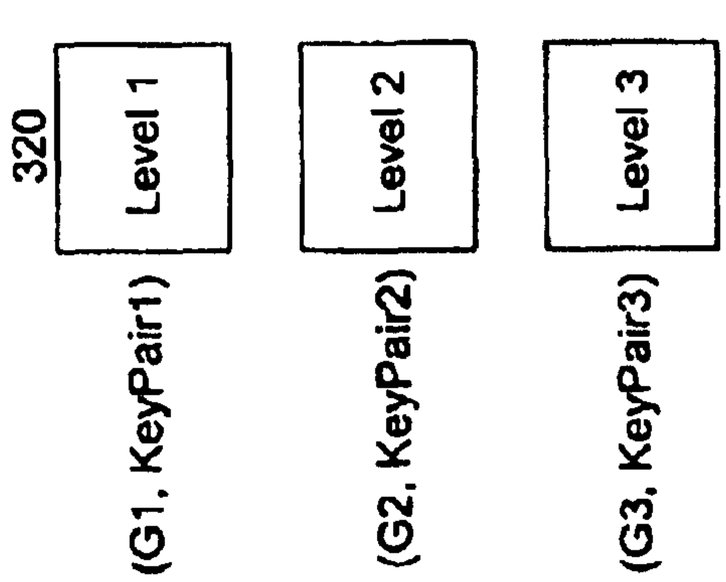

324
Level 1
{U1, KeyPair1}
Level 3
{U3, KeyPair3, U2, KeyPair2}
Fold into a next lower level

FIG. 3C


320
Level 1
(G1, KeyPair1)
Level 2
(G2, KeyPair2)
Level 3
(G3, KeyPair3)

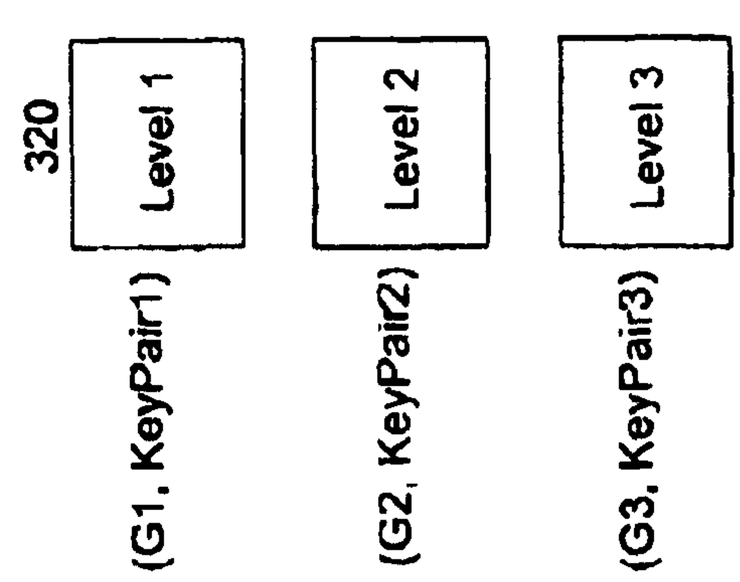
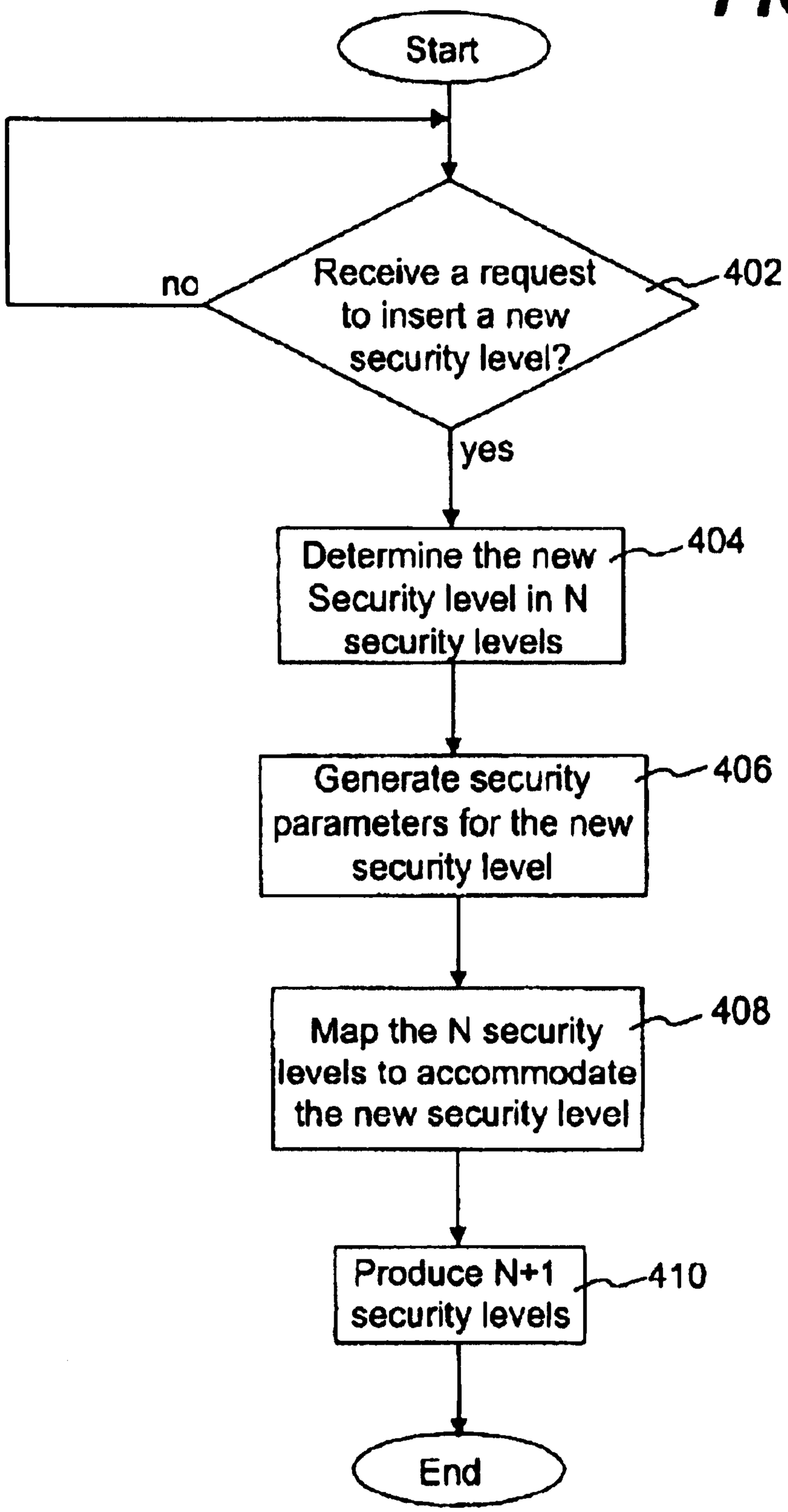

320
Level 1
(G1, KeyPair1)
Level 2
(G2, KeyPair2)
Level 3
(G3, KeyPair3)

FIG. 4A


Start
Receive a request to insert a new security level?
402
no
yes
Determine the new Security level in N security levels
404
Generate security parameters for the new security level
406
Map the N security levels to accommodate the new security level
408
Produce N+1 security levels
410
End

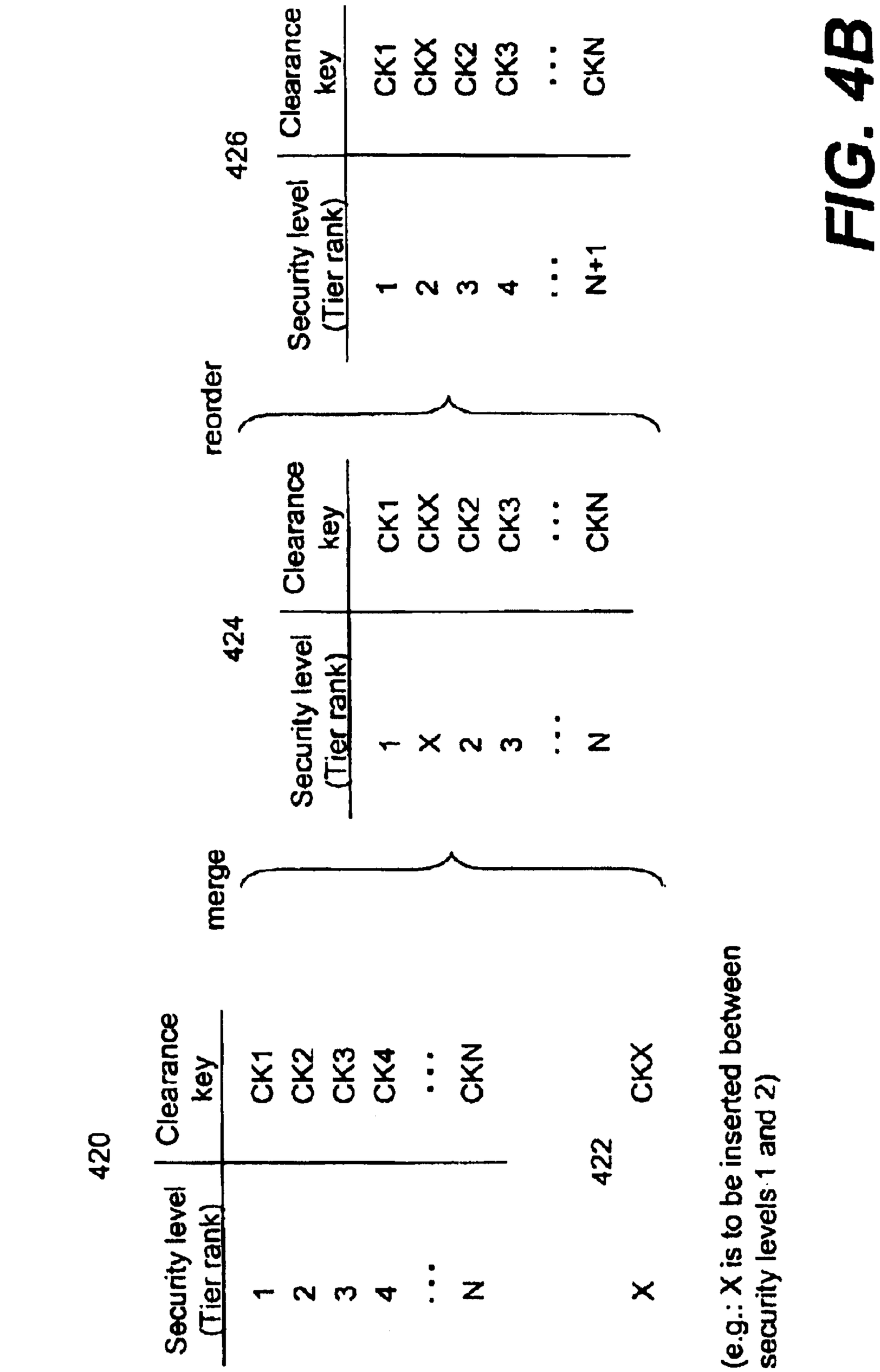
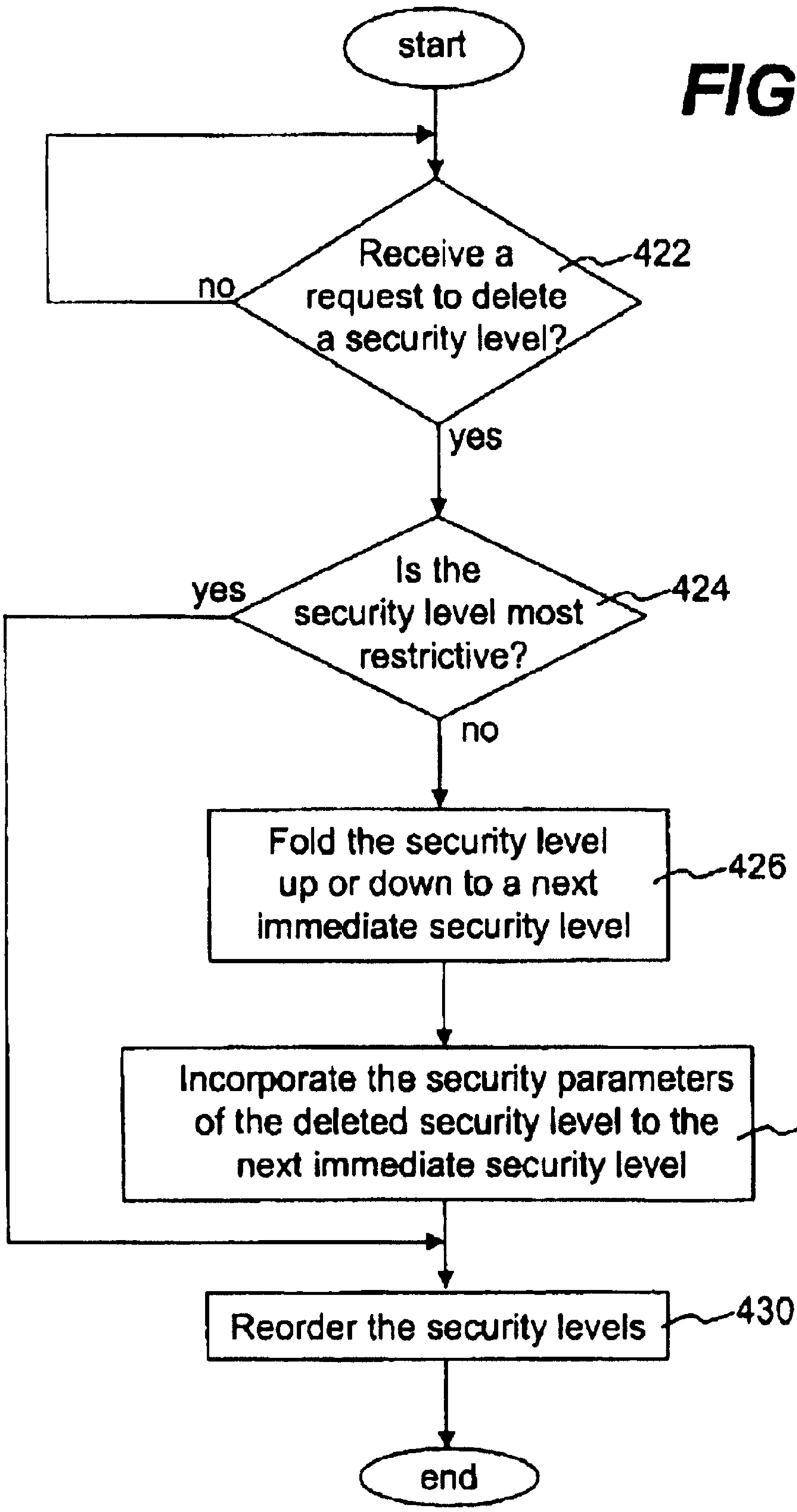

420
Security level (Tier rank)
Clearance key
1 CK1
2 CK2
3 CK3
4 CK4
... ...
N CKN
422
X CKX
(e.g.: X is to be inserted between security levels 1 and 2)
merge
424
Security level (Tier rank)
Clearance key
1 CK1
X CKX
2 CK2
3 CK3
... ...
N CKN
reorder
426
Security level (Tier rank)
Clearance key
1 CK1
2 CKX
3 CK2
4 CK3
... ...
N+1 CKN

FIG. 4B

FIG. 4C


start
Receive a request to delete a security level?
422
no
yes
Is the security level most restrictive?
424
yes
no
Fold the security level up or down to a next immediate security level
426
Incorporate the security parameters of the deleted security level to the next immediate security level
428
Reorder the security levels
430
end

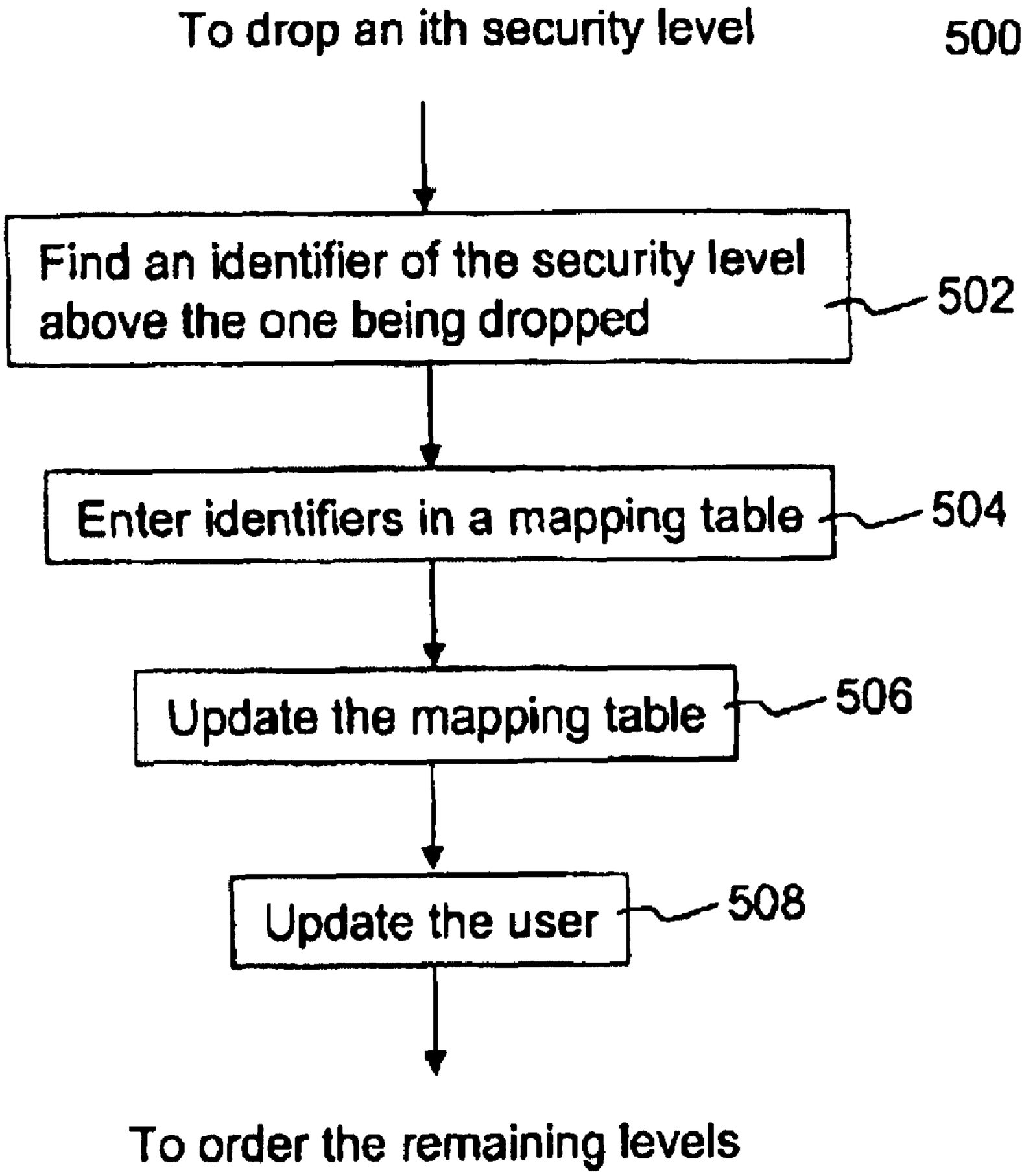

To drop an ith security level
500
Find an identifier of the security level above the one being dropped
502
Enter identifiers in a mapping table
504
Update the mapping table
506
Update the user
508
To order the remaining levels

FIG. 5A

510

Identifier	Level	C Key	Comments
B5C	1	CK1	Top secret
A92	2	CK2	Very secret
FF5	3	CK3	Secret
CD7	4	CK4	Confidential
...	...	...	...
B5C	N	CKN	Insignificant

FIG. 5B

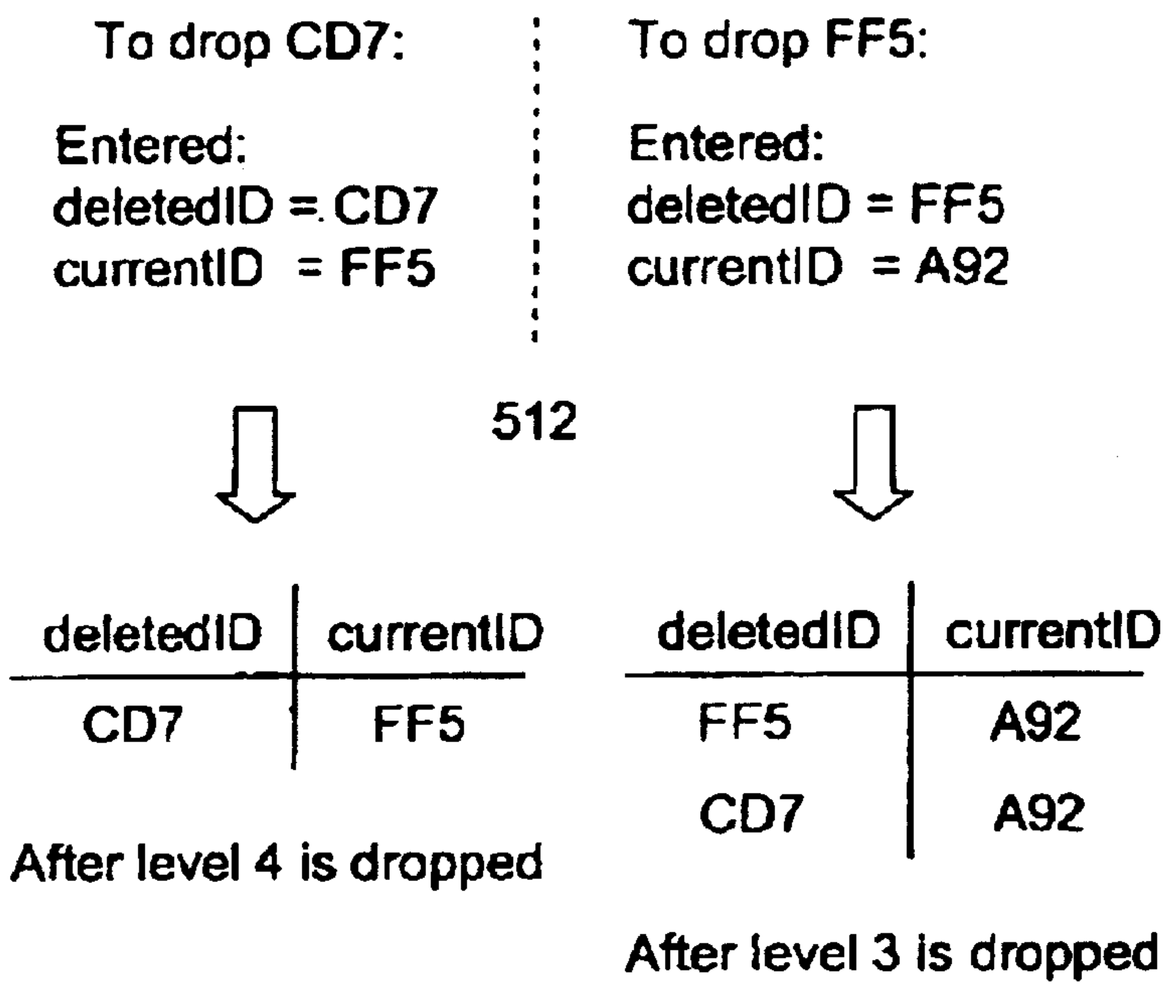


FIG. 5C

METHOD AND SYSTEM FOR MANAGING SECURITY TIERS

Matter enclosed in heavy brackets [ ] appears in the original patent but forms no part of this reissue specification; matter printed in italics indicates the additions made by reissue.

CROSS-REFERENCE TO RELATED APPLICATION

This application is a continuation-in-part of co-pending U.S. patent application Ser. No. 10/076,254, filed Feb. 12, 2002, that claims the benefits of U.S. provisional application No. 60/339,634 filed Dec. 12, 2001. The application is also related to U.S. patent application Ser. No. 10/159,537 and entitled "Method and Apparatus for Securing Digital Assets", which is hereby incorporated by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to the area of protecting data in an enterprise environment, and more particularly, relates to a method and system for managing security tiers or levels without implicating accessibilities to secured files classified according to a security level.

2. Description of Related Art

The Internet is the fastest growing telecommunications medium in history. This growth and the easy access it affords have significantly enhanced the opportunity to use advanced information technology for both the public and private sectors. It provides unprecedented opportunities for interaction and data sharing among businesses and individuals. However, the advantages provided by the Internet come with a significantly greater element of risk to the confidentiality and integrity of information. The Internet is a widely open, public and international network of interconnected computers and electronic devices. Without proper security means, an unauthorized person or machine may intercept any information traveling across the Internet and even get access to proprietary information stored in computers that interconnect to the Internet, but are otherwise generally inaccessible by the public.

There are many efforts in progress aimed at protecting proprietary information traveling across the Internet and controlling access to computers carrying the proprietary information. Cryptography allows people to carry over the confidence found in the physical world to the electronic world, thus allowing people to do business electronically without worries of deceit and deception. Every day hundreds of thousands of people interact electronically, whether it is through e-mail, e-commerce (business conducted over the Internet), ATM machines, or cellular phones. The perpetual increase of information transmitted electronically has lead to an increase reliance on cryptography.

One of the ongoing efforts in protecting the proprietary information traveling across the Internet is to use one or more cryptographic techniques to secure a private communication session between two communicating computers on the Internet. The cryptographic techniques provides a way to transmit information across an insecure communication channel without disclosing the contents of the information to anyone eavesdropping on the communication channel. Using an encryption process in a cryptographic technique, one party can protect the contents of the data in transit from access by an unauthorized third party yet the intended party can read the data using a corresponding decryption process.

A firewall is another security measure that protects the resources of a private network from users of other networks. However, it has been reported that many unauthorized accesses to proprietary information occur from the inside, as opposed to from the outside. An example of someone gaining unauthorized access from the inside is when restricted or proprietary information is accessed by someone within an organization who is not supposed to do so. Due to the open nature of the Internet, contractual information, customer data, executive communications, product specifications, and a host of other confidential and proprietary intellectual property, remains available and vulnerable to improper access and usage by unauthorized users within or outside a supposedly protected perimeter.

In fact, many businesses and organizations have been looking for effective ways to protect their proprietary information. Typically, businesses and organizations have deployed firewalls, Virtual Private Networks (VPNs), and Intrusion Detection Systems (IDS) to provide protection. Unfortunately, these various security means have been proven insufficient to reliably protect proprietary information residing on private networks. For example, depending on passwords to access sensitive documents from within often causes security breaches when the password of a few characters long is leaked or detected. Therefore, there is a need to provide more effective ways to secure and protect digital assets at all times.

When a security system is employed to secure files, it is sometimes desirable to classify the secured files according to a security level, for example, "top secret", "secret" or "confidential". When there is a need to add or delete additional security levels, the secured files originally classified should be still accessible. Thus there is a need for solutions that can manage the security levels dynamically without implicating accessibility to the secured files.

SUMMARY OF INVENTION

This section is for the purpose of summarizing some aspects of the present invention and to briefly introduce some preferred embodiments. Simplifications or omissions in this section as well as in the abstract may be made to avoid obscuring the purpose therefor. Such simplifications or omissions are not intended to limit the scope of the present invention.

The present invention is related to processes, systems, architectures and software products for providing pervasive security to digital assets at all times and is particularly suitable in an inter/intra enterprise environment. In general, pervasive security means that digital assets are secured at all times and can only be accessed by authenticated users with appropriate access rights or privileges, and proper security clearance in some cases, wherein the digital assets may include, but not be limited to, various types of documents, multimedia files, data, executable code, images and texts. According to one aspect of the present invention, secured files are in a secured form that only those with granted access rights can access. Even with the proper access privilege, when a secured file is classified, at least a security clearance key is needed to ensure those who have the right security clearance can ultimately access the contents in the classified secured file.

According to one aspect of the present invention, a new security level is to be inserted into a set of existing security levels. For example, a security level "secret" is added between the existing security levels "top secret" and "confidential", resulting in a new set of security levels, "top

secret", "secret" and "confidential". Without implicating the accessibility to secured files classified at one of the existing security levels, the controllability or restrictiveness of the new security level is determined with respect to the most restrictive security level or the least security level in the existing security levels. A set of proper security parameters are generated for the new security level and subsequently the existing security levels are mapped to accommodate the new security level.

According to another aspect of the present invention, a security level is removed from a set of existing security levels. For example, a security level "secret" is removed from the existing security levels "top secret", "secret" and "confidential", resulting in a new set of security levels including only "top secret" and "confidential". Without implicating the accessibility to secured files classified at one of the existing security levels, the security parameters for the security level to be deleted are either folded up or down to an immediate next security level, depending on implementation. As a result, the security parameters for the immediate next security level are augmented to include those for the security level to be deleted such that the secured files classified at the security level to be deleted can still be accessed by those with proper clearance levels.

Depending on implementation and application, the present invention may be implemented in software, hardware or both in combination, and employed in a client machine or a server machine. According to one embodiment, the present invention is implemented in an executable form loaded in a computing device and activated when the security tiers or levels are changed to provide particular needs of an organization or organizations.

The present invention can be implemented as a method, a system, a process, software medium or other form, each yielding one or more of the following features, benefits and advantages. One of the features, benefits and advantages is the management mechanism of security levels in a security system, the mechanism provides flexibility in reorganizing security levels without implicating accessibility to secured files originally classified. Another one of the features, benefits and advantages is that secured files originally classified at a security level to be deleted can still be accessed by properly folding the security level to a next immediate security level.

Other objects, features, and advantages of the present invention will become apparent upon examining the following detailed description of an embodiment thereof, taken in conjunction with the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features, aspects, and advantages of the present invention will become better understood with regard to the following description, appended claims, and accompanying drawings where:

FIG. **1** shows a diagram of securing a created document according to one exemplary secured file form used in the present invention;

FIG. **2**A shows a diagram of what is referred to herein as a two-pronged access scheme according to one embodiment of the present invention;

FIG. **2**B shows a flowchart of a process for granting a proper security clearance level (i.e., a clearance key) according to one embodiment of the present invention;

FIG. **2**C shows a diagram of generating a clearance key according to one embodiment of the present invention;

FIG. **2**D shows a diagram of generating a clearance key according to another embodiment of the present invention;

FIG. **3**A illustrates a set of security levels in a security system employed in an enterprise, a new security level being inserted to the existing security level;

FIG. **3**B and FIG. **3**C each illustrate a case in which a security level is folded into another security level;

FIG. **4**A shows a flowchart or process of inserting a new security level into N security levels according to one embodiment of the present invention;

FIG. **4**B shows a flowchart or process of deleting a security level out of N security levels according to one embodiment of the present invention;

FIG. **4**C shows a flowchart or process of deleting a security level out of N security levels according to one embodiment of the present invention;

FIG. **5**A shows an exemplary implementation of dropping an ith level out of N existing level by folding the ith level to (i—i)th level and may be understood in conjunction with FIG. **5**B and FIG. **5**C;

FIG. **5**B shows a table listing identifiers, levels, clearance keys and corresponding literal meanings according to one embodiment; and

FIG. **5**C shows a clearance mapping table being entered and updated.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention pertains to a process, a system, a method and a software product for securing electronic data or digital assets. According to one aspect of the present invention, a new security level is to be inserted into a set of existing security levels. Without implicating the accessibility to secured files classified at one of the existing security levels, the controllability or restrictiveness of the new security level is determined with respect to the most restrictive security level or the least security level in the existing security levels. A set of proper security parameters are generated for the new security level and subsequently the existing security levels are mapped to accommodate the new security level. According to another aspect of the present invention, a security level is removed from a set of existing security levels. The security parameters for the security level to be deleted are either folded up or down to an immediate next security level, depending on implementation. As a result, the security parameters for the immediate next security level are augmented to include those for the security level to be deleted such that the secured files classified at the security level to be deleted can still be accessed by those with proper clearance levels.

There are numerous advantages, benefits, and features in the present invention. One of them is the mechanism contemplated herein capable of providing pervasive security to digital assets sought to be protected at all times. Another one is that the digital assets are presented in such a way that only those with proper access privilege as well as sufficient security clearance level can access information in the digital assets. Other advantages, benefits, and features in the present invention can be readily appreciated by those skilled in the art from the detailed description of the invention provided herein.

In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will become obvious to those skilled in the art that the present invention may be practiced

without these specific details. The description and representation herein are the common means used by those experienced or skilled in the art to most effectively convey the substance of their work to others skilled in the art. In other instances, well-known methods, procedures, components, and circuitry have not been described in detail to avoid unnecessarily obscuring aspects of the present invention.

Reference herein to "one embodiment" or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment can be included in at least one embodiment of the invention. The appearances of the phrase "in one embodiment" in various places in the specification are not necessarily all referring to the same embodiment, nor are separate or alternative embodiments mutually exclusive of other embodiments. Further, the order of blocks in process flowcharts or diagrams representing one or more embodiments of the invention do not inherently indicate any particular order nor imply any limitations in the invention.

Embodiments of the present invention are discussed herein with reference to FIGS. **1**–**4**B. However, those skilled in the art will readily appreciate that the detailed description given herein with respect to these figures is for explanatory purposes as the invention extends beyond these limited embodiments.

Generally, a content created by a creator for the purpose of an entity is an intellectual property belonging to the creator or the entity. In an enterprise, any kind of information or intellectual property can be content, though it is commonly referred to as "information" instead of "content". In either case, content or information is independent of its format, it may be in a printout or an electronic document. As used herein, content or information exists in a type of electronic data that is also referred to as a digital asset. A representation of the electronic data may include, but not be limited to, various types of documents, multimedia files, streaming data, dynamic or static data, executable code, images and texts.

To prevent contents in electronic data from an unauthorized access, the electronic data is typically stored in a form that is as close to impossible as possible to read without a priori knowledge. Its purpose is to ensure privacy by keeping the content hidden from anyone for whom it is not intended, even those who have access to the electronic data. Example of a priori knowledge may include, but not be limited to, a password, a secret phase, biometric information or one or more keys.

FIG. **1** shows an illustration diagram of securing a created document **100** according to one embodiment of the present invention. One of the purposes of creating a secured file **108** is to ensure that the contents in the document **100** can be only accessed by or revealed to an authorized user with proper access privilege. As used herein, the user may mean a human user, a software agent, a group of users or a member thereof, a device and/or application(s). Besides a human user who needs to access a secured document, a software application or agent sometimes needs to access the secured document in order to proceed forward. Accordingly, unless specifically stated, the "user" as used herein does not necessarily pertain to a human being.

After the document **100** is created, edited or opened with an application or authoring tool (e.g., Microsoft WORD), upon an activation of a command, such as "Save," "Save As" or "Close", or automatic saving invoked by an operating system, the application itself, or an approved application, the created document **100** is caused to undergo a securing process **101**. The securing process **101** starts with an encryption process **102**, namely the document **100** that has been created or is being written into a store is encrypted by a cipher (e.g., an encryption process) with a file key (i.e., a cipher key). In other words, the encrypted data portion **112** could not be opened without the file key. For the purpose of controlling the access to the contents in the document **100** or the resultant secured file **108**, the file key or keys may be the same or different keys for encryption and decryption and are included as part of security information contained in or pointed to by a header **106**. The file key or keys, once obtained, can be used to decrypt the encrypted data portion **112** to reveal the contents therein.

To ensure that only authorized users or members of an authorized group can access the secured file **108**, a set of access rules **104** (an example is shown in the figure) for the document **100** is received or created and associated with the header **106**. In general, the access rules **104** determine or regulate who and/or how the document **100**, once secured, can be accessed. In some cases, the access rules **104** also determine or regulate when or where the document **100** can be accessed. In addition, security clearance information **107** is added to the header **106** if the secured file **108** is classified. In general, the security clearance information **107** is used to determine a level of access privilege or security level of a user who is attempting to access the contents in the secured file **108**. For example, a secured file may be classified as "Top secret", "Secret", "Confidential", and "Unclassified".

According to one embodiment, the security clearance information **107** includes another layer of encryption of the file key with another key referred to herein as a clearance key. An authorized user must have a clearance key of proper security level in addition to an authenticated user key and proper access privilege to retrieve the file key. As used herein, a user key or a group key is a cipher key assigned to an authenticated user and may be used to access a secured file or secure a file, or create a secured file. The detail of obtaining such a user key upon a user being authenticated is provided in U.S. patent application Ser. No. 10/074,804.

According to another embodiment, the security clearance information **107** includes a set of special access rules to guard the file key. The retrieval of the file key requires that the user passes an access rule measurement. Since access privilege of a user may be controlled via one or more system parameters (e.g., a policy), the access rule measurement can determine if the user has sufficient access privilege to retrieve the file key in conjunction with the corresponding user key. With the detailed description to follow, those skilled in the art can appreciate that other forms of the security clearance information **107** may be possible. Unless otherwise specified, the following description is based on the security clearance information **107** being another layer of encryption with one or more clearance keys.

In accordance with the security clearance information **107**, a user may be assigned a hierarchical security clearance level based on, perhaps, a level of trust assigned to the user. A level of trust implies that one user may be more trusted than another and hence the more trusted user may access more classified files. Depending on implementation, a level of trust may be based on job responsibility of the user or a role of the user in a project or an organization background checks, psychological profiles, or length of service, etc. In any case, a level of trust assigned to the user augments additional aspect to the access privilege of the user such that the user must have proper security clearance to access a classified secured file even if the user is permitted by the access rules to access the file.

As will be further described in detail below, unless the level of security clearance of the user permits, a secured classified file (i.e., the file that is both secured and classified) may not be accessed even if the user has an authenticated user (or group) key and permitted by the access rules in the secured classified file. In one embodiment, the level of security clearance of the user is determined by one or more clearance keys assigned thereto. In general, a clearance key permits a user to access a secured file classified as "top secret", the same clearance key may permit the user to access all secured files classified less secure, such as "secret" or "confidential", where it has been assumed that the user has proper access privilege to be granted by the access rules in the file. In one embodiment, a clearance key is further secured by means of secondary authentication, such as re-login, biometric information verification and a second password. In other words, a clearance key may not be automatically released to or activated for a user upon an authenticated login, unless the user provides additional information.

In general, a header is a file structure, preferably small in size, and includes, or perhaps links to, security information about a resultant secured document. Depending on an exact implementation, the security information can be entirely included in a header or pointed to by a pointer that is included in the header. According to one embodiment, the access rules **104**, as part of the security information, are included in the header **106**. The security information further includes the file key and/or one or more clearance keys, in some cases, an off-line access permit (e.g. in the access rules) should such access be requested by an authorized user. The security information is then encrypted by a cipher (i.e., an en/decryption scheme) with a user key associated with an authorized user to produce encrypted security information **110**. The encrypted header **106**, if no other information is added thereto, is attached to or integrated with the encrypted data portion **112** to generate the resultant secured file **108**. In a preferred embodiment, the header is placed at the beginning of the encrypted document (data portion) to facilitate an early detection of the secured nature of a secured file. One of the advantages of such placement is to enable an access application (i.e., an authoring or viewing tool) to immediately activate a document securing module (to be described where it deems appropriate) to decrypt the header if permitted. Nevertheless, there is no restriction as to where the encrypted header **106** is integrated with the encrypted data portion **112**.

It is understood that a cipher may be implemented based on one of many available encryption/decryption schemes. Encryption and decryption generally require the use of some secret information, referred to as a key. For some encryption mechanisms, the same key is used for both encryption and decryption; for other mechanisms, the keys used for encryption and decryption are different. In any case, data can be encrypted with a key according to a predetermined cipher (i.e., encryption/decryption) scheme. Examples of such schemes may include, but not be limited to, Data Encryption Standard algorithm (DES), Blowfish block cipher and Twofish cipher. Therefore, the operations of the present invention are not limited to a choice of those commonly-used encryption/decryption schemes. Any cipher scheme that is effective and reliable may be used. Hence, the details of a particular scheme are not further discussed herein so as to avoid obscuring aspects of the present invention.

In essence, the secured document **108** includes two parts, the encrypted data portion **112** (i.e., encrypted version of the document itself) and the header **110** that may point to or include security information for the secured document **108**. To access the contents in the encrypted data portion **112**, one needs to obtain the file key to decrypt the encrypted data portion **112**. To obtain the file key, one needs to be authenticated to get a user or group key and pass an access test in which at least the access rules in the security information are measured against the user's access privilege (i.e., access rights). If the secured file is classified, it further requires a security level clearance on the user. In general, the security clearance level of the user must be high enough before the file key can be retrieved. Alternatively, part of the access rules may be left non-encrypted for users authorized or non-authorized alike to view embedded access permissions of a secured file in a display application or markup language interpreter (e.g., a browser).

FIG. **2**A shows a diagram **200** of what is referred to herein as a two-pronged access scheme according to one embodiment of the present invention. To access a secured file **201**, a user needs to have access privilege based on a condition of "need to know" **202** that is to be measured against by the access rules **204** embedded in the secured file **201**. If the secured file **201** is classified, the user must also have a higher security clearance level **206** that is measured against by the security clearance information **206** (e.g., one or more clearance keys. In other words, there are at least two key holes **210** that must be "inserted" with two proper keys before the secured classified file can be accessed.

FIG. **2**B shows a flowchart **220** of process for granting a proper security clearance level (i.e., a clearance key) according to one embodiment of the present invention. The process **220** can be initiated with a request for a clearance key. Depending on implementation, the process **220** may be implemented in a machine (e.g., a central server, a local server or a client machine) that provides access control management to all secured files, perhaps, in an inter/intra enterprise environment, or a combination of a local client machine used by users and the machine.

At **222**, the process **220** awaits a request for a clearance key. It is described that a secured file can be classified or unclassified. When it is determined that a user needs to access a secured file that is classified at a security level, such request is provided to activate the process **220**. In general, the request pertains to a specific user or some members in a group. At **224**, a corresponding account for the user is retrieved, provided there is the account for the user. If the account is not available, then the account shall be opened accordingly. Alternatively, the process **220** may be part of the process of opening an appropriate account for a user who has the need-to-know basis to access secured files at certain security or confidential level(s). Depending on implementation, the corresponding account information may include a username or identifier, membership information, designated access privilege, and a corresponding user key (which sometimes is a pair of a private key and a public key). At **226**, a security level for the user is determined, which is usually done by the necessity. For example, an executive of an enterprise may be assigned the highest security clearance level and a front desk receptionist may be assigned the lowest security clearance level. Once the security level is determined, a clearance key is generated at **228**.

Referring now to FIG. **2**C, there is shown a diagram **240** of generating a clearance key according to one embodiment of the present invention. A key generator **244** receives one or more parameters **242** controlling the security level determined at **226** of FIG. **2**B to generate a sequence of alpha-numeric characters or binary numbers as a key. Whether

using a secret-key cryptosystem or a public-key cryptosystem, one needs a good source of random numbers for key generation. The main features of a good source are that it produces numbers that are unknown and unpredictable by potential adversaries. There are many ways to generate such numbers, for example, random numbers can be obtained from a physical process. Another approach is to use a pseudo-random number generator fed by a random seed. In any case, depending on the input **242**, the generator **244** is configured to generate a clearance key of proper security level. In one embodiment, the key generator **244** generates keys **246** of different lengths or forms, each of the keys **246** corresponds to a security level, such as level **1** (highest security), level **2**, . . . , level N (lowest security). In another embodiment, each of the keys **246** generated by the key generator **244** is embedded with a signature signifying a security level. Other methods of specifying a security level of a clearance key are possible. Although it is possible to implement in such a way that each clearance key with a certain security level can only access secured files classified in the same security level, it is preferable to permit a clearance key with a higher security level to access secured files classified in the lower security levels. In other words, a clearance key in level **1** (i.e., the highest security level primarily designated to secured files classified as "top secret") can be used to access all secured classified files **248**, while a clearance key in level **2** can be used to access all secured classified files **248** except for those classified as "top secret". Likewise, a clearance key in level N can be only used to access secured files in security level N. One of the advantages for such arrangement is that a user needs only to have one clearance key, if the user has the need to access those secured classified files.

FIG. **2**D shows a diagram of generating a clearance key according to another embodiment of the present invention. The key generator **244** receives one or more parameters **242** controlling the security level determined at **226** of FIG. **2**B to generate a number of sets of alphanumeric or binary numbers as a primary key **246** and auxiliary keys **247**. The primary key **246** is the one being requested, generated in accordance with the determined security level and can be used to facilitate the access to a secured file classified at a security or confidentiality level. The auxiliary keys are those keys generated to facilitate the access to secured files classified less than the security or confidentiality level. As shown in the figure, it is assumed that the primary key **246** is for accessing a secured file classified at level **2**. Accordingly, the auxiliary keys **247** can be respectively used to access secured files classified level **3**, level **4**, . . . to level N, all less than level **2** in terms of security or confidentiality. To facilitate the description of the present invention, the following description is based on FIG. **2**C and can be readily applied to FIGS. **2**D.

Returning to FIG. **2**B, after a proper clearance key is generated at **228**, the clearance key is associated with the account at **230** so that the user will use the correct key to access a secured file that requires a clearance key. The process **220** now awaits any call for the clearance key at **232**. Depending on implementation, the clearance key may be stored locally or remotely and retrievlable only when there is a need for it to access a classified secured file. In some cases, the clearance key can only be retrievlable when a user passes a secondary authentication means. For example, a user is entitled to access certain secured files classified at least at a security level. The clearance key associated with the user may be configured to be protected by means of secondary authentication, such as biometric information verification or a second password, to increase security level of the clearance key. When a non-secured classified file is accessed, the clearance key is not needed and therefore will not be released to or activated for the user. When a secured classified file is accessed, the process **220** goes to **234**, wherein the clearance key is released to the user to facilitate the retrieval of the file key in the secured file, provided the user has furnished necessary information or passed secondary authentication if needed.

Clearance keys provide flexibilities for a security system to control access by authorized users to secured files that are classified accordingly. However, when levels of the security are fixed, the flexibilities are limited. As one of the features in the present invention, the levels of security can be added or adjusted up or down in a security system without compromising the security of the secured files that have been previously classified.

FIG. **3**A illustrates security levels **302** in a security system employed in an enterprise. In general, there are N levels of security for secured files under the security system, where N is a finite integer, each level requires a set of security parameters to access secured files classified to the level or other levels below this level. For example, a secured file SF is classified at security level **2**. To access the secured file, users in a designated group G**2** shall posses at least two keys, a user key (e.g., UK**2**) and a clearance key (e.g., CK**2**) corresponding to the security level **2**. The designated group includes a user or users authorized to access the secured files classified at this level or levels below this level. The user key for each of the users, if there are more than one users in the designated group, may not be necessary identical, as one user may be from one user group and another user may be from a different group. To facilitate the description of the present invention, the access relationship may be expressed as: SF ∀ (group, security-level, CK), which means a secured and classified file SF can be accessed with valid parameters of a designated group, a security-level, a clearance key. In particular, SF ∀ (G**2**, level2, C<) means that users in a group designated as G**2** can access secured file classed at level **2** with a clearance key CK**2**, provided that each of the users in G**2** has a valid user key. Alternatively, SF ∀ (G**2**, level1, level2, CK**2**) means that users in a group designated as G**2** can access secured files classified at level **1** or level **2** with a clearance key CK**2**, provided that each of the users in G**2** has a valid user key. The first access relationship indicates that the secured file SF can only be accessed by users in a group G**2** authorized to access secured files classified at the security level **2**. The second access relationship indicates that secured files classified at the security level **2** or one level below the security level **2** can be accessed by users authorized to access secured files classified at the security level **2**. Depending on implementation, either one of the access relationships may be implemented.

For simplified illustration purpose, the first access relationship is shown in the figures and the following description is based on the first access relationship. Those skilled in the art can understand the implementation of the second access relationship given the detailed description herein. When an additional security level **304** is added between the security levels **1** and **2**, the groups and corresponding keys have to be reassigned without affecting the accessibility to other secured files originally classified. According to one embodiment, the security level **1** is the most restrictive level. Since the added level **304** is less restrictive than the security level **1** but more restrictive than level **2**, as shown in FIG. **3**A, the added level **304** is thus classified as a new security level **2** **308**. As a result, the rest of the original security levels,

except for the security level **1**, are reorganized, creating N+**1** levels of security **310** and a new access relationship SF ∀ (GX, level **2**, CKX), where GX is a newly authorized group to be permitted to access secured files at the security level **2** with a user key and the newly created clearance key CKX.

To maintain the accessibility of the originally authorized groups, the security levels are renumbered or remapped. If the original access relationship is SF ∀ (G**2**, level **2**, CK**2**), there is now SF ∀ (G**3**, level **3**, CK**2**), namely the original security level **2** is mapped to as security level **3**.

FIG. **3**B and FIG. **3**C each illustrate a case in which a security level is folded into another security level. Originally, there are three security levels **320**. Now the three security levels **320** are to be folded into two security levels **322** or **324**. FIG. **3**B shows the security levels **320** being folded up to an immediate next security level above, and FIG. **3**C shows the security levels **322** being folded down to an immediate next security level below. In particular, in FIG. **3**B, the security level **2** is to be folded into the security level **1**, a higher security level. As a result of one security level being folded up, there are now two security levels **322**. The authorization (i.e., security parameters) designated for the deleted security level (i.e., security level **2**) need be merged with that for the security level **1**. In other words, the original access relationships:

SF ∀ (G**1**, level **1**, CK**1**);

SF ∀ (G**2**, level **2**, CK**2**);

SF ∀ (G**3**, level **3**, CK**3**);

are now correspondingly mapped to:

SF ∀ (G**1**, level **1**, CK**1**, G**2**, level **2**, CK**2**);

SF ∀ (G**3**, level **3**, CK**3**).

In other words, those secured files classified at security level **2** can still be accessed by those with proper access privilege.

One the other hand, FIG. **3**C shows the security level **2** is being folded to the security level **3**. The authorization (i.e., security parameters) designated for the deleted security level (i.e., security level **2**) need be merged with that for the security level **3**. In other words, the original access relationships:

SF ∀ (G**1**, level **1**, CK**1**);

SF ∀ (G**2**, level **2**, CK**2**);

SF ∀ (G**3**, level **3**, CK**3**);

are now correspondingly mapped to:

SF ∀ (G**1**, level **1**, CK**1**);

SF ∀ (G**3**, level **3**, CK**3**, G**2**, level **2**, CK**2**).

In other words, those secured files classified at security level **2** can still be accessed by those with proper access privilege.

FIG. **4**A shows a flowchart or process **400** of inserting a new security level into N security levels according to one embodiment of the present invention. The process **400** can be implemented in software, hardware or both of software and hardware. In a typical application, the process **400** is executed in a security system employed to manage secured files for an enterprise or a group of collaborative business entities.

At **402**, the process **400** awaits a request to insert a new security level into N existing security levels. For example, a system was configured to manage secured files classified respectively in accordance with one of N security levels. In other words, there are N security levels in the system. For some reason, the system needs to be configured to manage N+1 security levels, namely a security level is to be added into the N security levels. Upon receiving a request to insert the new security level, the process **400** determines how restrictive the new security level is with respect to the N security level at **404**. It is assumed that the 1 st security level in the N security levels is most restrictive while the Nth security level is least restrictive. The relative restrictiveness of the new security level is a relative position in the stack of the N security levels, indicating how less or more restrictive with respect to the 1 st security level or the Nth security level.

At **406**, a set of security parameters is generated for the new security level. The security parameters include at least a clearance key and a relative security level (e.g., a tier rank). The clearance key may be respectively generated in accordance with FIG. **2**C or FIG. **2**D or other means known to those skilled in the art. The clearance key is associated with the new security level, and a group of users are then authorized to access secured files classified at this new security level.

At **408**, the new security level is now created in the original N security levels, resulting N+1 security levels. Without implicating the accessibility to secured files classified at other security levels, the security levels below the new security level are mapped accordingly. For example, an ith security level in the original N security levels now becomes an (i+1) security level and the corresponding security parameters are also shifted accordingly. In another perspective, SF ∀ (Gi, level i, CKi) is now SF ∀ (G(i+1), level (i+1), CKi). At **410**, a new set of security levels is created, which does not implicate the accessibility to secured files originally classified and the originally authenticated users are still able to access the secured files they are entitled to.

FIG. **4**B is provided to further understand FIG. **4**A with respect to one embodiment of the present invention and shows that a table **420** include clearance keys, each for a security level. A set of parameters **422** for a new security level X is generated. It is assumed that the new security level X is to be inserted between security levels **1** and **2**. The table **424** shows the relative position of the new security level in the original N security levels in a system. The table **426** shows reordering of the security levels to accommodate the new level that is now with a tier rank being 2 and the corresponding clearance keys are respectively associated with their original ranks. As a result, the secured files classified per the original security levels are still accessible.

According to one embodiment, when an authorized user logins into the system, with the login information in reference to a group, the user is granted at least two keys (a corresponding clearance key and a user key) such that the user can access secured files classified at the granted security level or any levels below this security level. According to another embodiment, when an authorized user logins into the system, with the login information in reference to a group, the user is granted all keys pairs the user is entitled to such that the user can access secured files classified at this security level or any levels below this security level. It should be noted that "granting" herein does not necessarily means only that the user receives the keys from the system. Depending on implementation, one or more of the keys or part or whole of the keys may be stored in a local or remote machine and caused to be activated for use only after the user is authenticated.

FIG. **4**C shows a flowchart or process **420** of deleting a security level out of N security levels according to one embodiment of the present invention. One of the features of the process **420** is to fold the deleted security level up or down to a next immediate security level so that users originally authorized to access secured files classified at the deleted security level can still access these secured files. The process **420** can be implemented in software, hardware or both of software and hardware. In a typical application, the process **420** is executed in a security system employed to

manage secured files for an enterprise or a group of collaborative business entities.

At **422**, the process **420** awaits a request to delete a security level out of N existing security levels. For example, a system was configured to manage secured files classified respectively in accordance with one of N security levels. In other words, there are N security levels in the system. For some reason, the system needs to be configured to manage N−**1** security levels, namely one of the N security levels is to be deleted. Upon receiving the request to delete, for example, an ith security level, the process **420** determines at **424** whether the ith security level is the most restrictive. It is assumed that the 1st security level in the N security levels is most restrictive while the Nth security level is least restrictive. Accordingly, the process **420** determines at **424** whether the security level to be removed is the 1st security level. If it is indeed the 1st security level, the request is denied.

It should be noted that **424** is not a limitation in the present invention and it can be folded down to a next immediate level. According to one embodiment, it is designed to suit in a more practical situation. In general, it is just not desirable to have a most restrictive security level to be deleted. In some other case, it is also not desirable to have a least restrictive security level to be deleted as well. Optionally, another checking may be employed in the process **420** to determine at **424** whether the security level to be removed is the Nth security level.

Depending on implementation, at **426**, the security level to be deleted is to be folded up or down to a next immediate security level. For example, an ith security level to be deleted can be merged with (i−1)th security level or (i+1)th security level. By merging the ith security level with its next immediate security level, it is possible to access those secured files classified at the ith security level even if this level is deleted.

To access those secured files classified at the ith security level, the security parameters, such as the keys and the group designations shall be retained. As a result, at **428**, the security parameters for the ith security level are transferred or updated accordingly. In general, for the case of folding up, the security parameters for the ith security level are merged with those for the (i−1)th security level, for the case of folding down, the security parameters for the ith security level are merged with those for the (i+1)th security level. At **430**, the security levels are reordered, for example from security levels **1** to N to **1** to (N−1).

FIG. **5**A shows an exemplary implementation **500** of dropping an ith level out of N existing levels by folding the ith level to (i—i)th level and may be understood in conjunction with FIG. **5**B and FIG. **5**C. A table **510** in FIG. **5**B shows that there are N security levels labeled as Level **1**, **2**, . . . ,N, where Level **1** is most restricted and Level N is least restricted. A security clearance key is associated with one of the security levels. Each of the security levels may mean literally a type of security, such as "top secret", "very secret", . . . "insignificant". Each of the N security levels is also identified by an identifier. According to one embodiment, the identifier is a sequence of digits (e.g. a hexadecimal number) generated in a system. For example in table **510**, the identifier B**5**C indicates security level **1**, and the identifier CD**7** indicates security level **4**. To facilitate the description of FIG. **5**A, it is assumed that the ith security level to be dropped is the security level **4**.

At **502**, an identifier of the security level above the one being dropped is located, namely the identifier of the (i−1)th security level. According to the table **510**, the identifier of the 3rd security level is FF**5** (i.e., currentID=FF**5**). Given the two identifiers FF**5** and C**07**, at **504**, these two identifiers are entered in a mapping table at **504**. FIG. **5**C shows a corresponding mapping table **512** which may be referred to as clearance mapping table, in which two IDs (deletedID and currentD) now have two entries, each being one of the two identifiers.

At **506**, the mapping table **512** is updated. There is no operation since there are any entries previously in the table **512**. At **508**, the user who is previously authorized to access secured files classified at CD**7** is updated. According to one embodiment, a notification is sent to the user or users who may have been affected by dropping CD**7** to cause the original clearance key (i.e., CK**4**) to be updated or exchanged with another clearance key (e.g., CD**3** for FF**5**). According to another embodiment, when a secured file classified at CD**7** is accessed, the original clearance key is used to access the file. At the time, the file is stored, saved or written back to a storage space, an updated clearance key (i.e., the key for FF**5**) is effectuated in accordance with CurrentID. In any case, the updating at **508** can be configured to be carried out transparently.

Next, it is assumed that another security level, Level **3**, is to be dropped. Accordingly, at **502**, the identifier (A**92**) of the security level above Level **3** is located. At **504**, these two identifiers are entered, namely deletedID=FF**5** and currentD=A**92**. At **506**, the table **512** needs to be updated. Since there is are entries from a previous deletion of one security level, these entries are preferably updated, thus the CurrentID is assigned to be A**92** as well as shown in FIG. **5**C. The affected user or users are updated at **508** so that these users can still access the secured files classified at FF**5**.

FIGS. **5**A, **5**B and **5**C show one exemplary implementation of folding up one deleted security level. Given the detailed description herein, other implementations including those to fold down a deleted security level can be readily developed by those skilled in art.

There are numerous features, advantages and benefits in the present invention. One of them is the mechanism provided to regroup security levels per a specific requirement without implicating the accessibility to secured files classified in accordance with the existing security levels. Another one of them is that a security level can be removed from a set of existing security levels while the security parameters for the security level to be deleted are either folded up or down to an immediate next security level. As a result, the security parameters for the immediate next security level are augmented to include those for the security level to be deleted such that the secured files classified at the security level to be deleted can still be accessed by those with proper clearance levels. Other features, advantages and benefits may be appreciated by those skilled in the art in the foregoing descriptions.

The present invention has been described in sufficient details with a certain degree of particularity. It is understood to those skilled in the art that the present disclosure of embodiments has been made by way of examples only and that numerous changes in the arrangement and combination of parts may be resorted without departing from the spirit and scope of the invention as claimed. Accordingly, the scope of the present invention is defined by the appended claims rather than the foregoing description of embodiments.

I claim:

1. **[**In a system for providing restrictive access to contents in secured files, each of the secured files classified in accordance with one of N security levels, a**]** *A* method for reorganizing **[**the**]** N security levels without implicating accessibilities to **[**the**]** secured files, *each of the secured files*

classified in accordance with one of the N security levels, the method comprising:

determining, *using a computing device,* a new security level with respect to the N security levels, wherein a 1st security level is most restrictive and an Nth security level is least restrictive **[**in**]** *among* the N security levels;

generating, *using the computing device,* security parameters accordingly for the new security level, the new security level being ith less restrictive with respect to the 1st security level; and

mapping, *using the computing device, an* ith security level in the N security levels to *an* (i+1)th security level in the N security levels to accommodate the new security level such that there are **[**now**]** (N+1) security levels in the system,

wherein each of the secured files includes an encrypted data portion and a security portion that controls restrictive access to the encrypted data portion, the security portion including a file key encrypted by at least a first key and a second key and further protected by a set of rules, and

wherein both of the first key and the second key must be obtained by a user whose access privilege is satisfied by the rules before the contents of the each of the secured files can be accessed.

2. The method of claim **1**, wherein the security parameters include**[**s**]** at least a clearance key and one or more of the parameters pertain to a designated group of users authorized to access the secured files classified at the new security level.

3. The method of claim **2**, wherein the clearance key is associated with the designated group of users, *and* together with a user key associated with each of the users, *allows access to* files secured at the ith security level **[**can now be accessed**]**.

4. The method of claim **2**, wherein, **[**when**]** *if* a user authorized to access secured files classified at the new security level **[**logins**]** *logs* into the system, the user is granted the clearance key, together with a user key **[**authorized**]** *authorizing* the user to access the secured files, **[**those**]** *and* secured files classified at the new security level can **[**now**]** be access*ed* by the user**[**s**]**.

5. The method of claim **4**, wherein**[**,**]** the clearance key is a private key in a pair of a public key and the private key, **[**those**]** *and the* secured files are classified at the new security *level* with the public key.

6. The method of claim **4**, wherein, if the user is authorized **[**at**]** *to access the* ith security level in the **[**original**]** N security levels, the user is **[**now**]** granted a *second* user key and a *second* clearance key such that the contents in the secured files classified at the (i+1)th security level and below can be **[**now**]** accessed by the user.

7. The method of claim **[6]** *1*, wherein the first key determines if the user is authorized to access the secured files classified at one of the N security levels or one of the (N+1) security levels, and the second key is in accordance with the one of the N security levels or the one of the (N+1) security levels.

8. **[**In a system for providing restrictive access to contents in secured files, at least some of the secured files classified in accordance with one of N security levels, a**]** *A* method for reorganizing **[**the**]** N security levels without implicating accessibilities to **[**the**]** secured files, *at least some of the secured files classified in accordance with one of the N security levels,* the method comprising:

upon receiving a request to remove an ith security level out of the N security levels, determining, *using a computing device,* if an (i−1)th security level is a 1st security level or if an (i+1)th security level is an Nth security level**[**s**]**, wherein the 1st security level is most restrictive and the Nth security level is least restrictive **[**in**]** *among* the N security levels;

[when**]** *if* the (i−1)th security level is not the 1st security level and the (i+1)th security level is not the Nth security level**[**s**]**, merging, *using the computing device,* the ith security level with either the (i−1)th security level or the (i+1)th security level such that there are **[**now**]** (N−1) security levels in the system,

wherein each of the secured files includes an encrypted data portion and a security portion that controls restrictive access to the encrypted data portion, the security portion including a file key encrypted by at least a first key and a second key and further protected by a set of rules, and wherein both of the first key and the second key must be obtained by a user whose access privilege is satisfied by the rules before the contents of **[**the**]** each of the secured files can be accessed.

9. The method of claim **8**, wherein users authorized to access secured files classified at the ith security level can **[**now**]** access secured files classified at the (i−1)th security level if the ith security level **[**is**]** *has been* merged with the (i−1)th security level.

10. The method of claim **8**, wherein users authorized to access secured files classified at the ith security level can **[**now**]** access secured files classified at the (i+1)th security level if the ith security level **[**is**]** *has been* merged with the (i+1)th security level.

11. The method of claim **8**, wherein at least two keys are needed to access secured files classified at the ith security level, *and* after the ith security level **[**is**]** *has been* merged with the (i−1)th or (i+1)th security level, the at lest two keys are incorporated into the (i−1)th or (i+1)th security level **[**as**]** such *that* users authorized to access the secured files classified at the ith security level can **[**still**]** access the secured files.

12. The method of claim **11**, wherein**[**, at the same time,**]** the users can access secured files classified at the (i−1)th or (i+1)th security level.

13. The method of claim **11**, wherein the at least two keys include a first key associated with a designated group of users and a second key being a clearance key in accordance with the ith security level.

14. The method of claim **13**, wherein, **[**when**]** *if* the user **[**logins**]** *logs* into the system, the user is granted the at least two keys.

15. The method of claim **8**, further comprising:

[when**]** *if* the (i−1)th security level is the 1st security level, denying the request to remove the ith security level out of the N security levels; or

always folding down the ith security level with (i−1)th security level.

16. The method of claim **8** further comprising:

[when**]** *if* the (i−1)th security level is the N security level, denying the request to remove the ith security level out of the N security levels; or

always folding up the ith security level with (i−1)th security level.

17. **[**In a**]** *A* system for providing restrictive access to contents in secured files, each of the secured files classified in accordance with one of N security levels, the system comprising:

a first machine loaded with a software module to reorganize the N security levels without implicating accessi-

bilities to the secured files, wherein the 1st security level is most restrictive and the Nth security level is least restrictive in the N security levels, [when] *and wherein, if* the software module is executed, the first machine performs operations of:

if a request [of] *for* deleting an ith security level out of the N security levels is received,

determining if an (i−1)th security level is a 1 st security level or if an (i+1)th security level is an Nth security level[s], wherein the 1st security level is most restrictive and the Nth security level is least restrictive in the N security levels; *and*

[when] *if* the (i−1)th security level is not the 1st security level and the (i+1)th security level is not the Nth security level[s], merging the ith security level with either the (i−1)th security level or the (i+1)th security level such that there are [now] (N−1) security levels in the system; and

if a request of adding a new security level into the N security is received,

determining a new security level with respect to the N security levels, wherein a 1 st security level is most restrictive and an Nth security level is least restrictive in the N security levels;

generating security parameters accordingly for the new security level, the new security level being ith less restrictive with respect to the 1st security level; *and*

mapping *an* ith security level in the N security levels to *an* (i+1)th security level in the N security levels to accommodate the new security level such that there are [now] (N+1) security levels in the system; and

a second machine, coupled to the first machine over a network, associated with a user that is granted with at least two keys to access one of the secured files classified at one of the N security levels,

wherein each of the secured files includes an encrypted data portion and a security portion that controls restrictive access to the encrypted data portion, the security portion including a file key encrypted by at least a first key and a second key and further protected by a set of rules, and

wherein both of the first key and the second key must be obtained by a user whose access privilege is satisfied by the rules before the contents of the each of the secured files can be accessed.

18. The system of claim **17**, wherein one of the two keys granted to the user is a clearance key in accordance with the one of the N security levels.

19. The system of claim **18**, wherein the two keys granted to the user are folded to either the (i−1)th security level or the (i+1)th security level, [when] *if* the user is authorized to access secured files classified at the ith security level.

20. A tangible computer-readable storage medium having stored thereon instructions that, if executed by a computing device, cause the computing device to perform a method comprising:

determining a new security level with respect to the N security levels, wherein a 1st security level is most restrictive and an Nth security level is least restrictive among the N security levels;

generating security parameters accordingly for the new security level, the new security level being ith less restrictive with respect to the 1st security level; and

mapping an ith security level in the N security levels to an (i+1)th security level in the N security levels to accommodate the new security level such that there are (N+1) security levels in the system,

wherein each of the secured files includes an encrypted data portion and a security portion that controls restrictive access to the encrypted data portion, the security portion including a file key encrypted by at least a first key and a second key and further protected by a set of rules, and

wherein both of the first key and the second key must be obtained by a user whose access privilege is satisfied by the rules before the contents of the each of the secured files can be accessed.

21. The computer-readable storage medium according to claim 20, wherein the security parameters include at least a clearance key and one or more of the parameters pertain to a designated group of users authorized to access the secured files classified at the new security level.

22. The computer-readable storage medium according to claim 21, wherein the clearance key is associated with the designated group of users, and together with a user key associated with each of the users, allows access to files secured at the ith security level.

23. The computer-readable storage medium according to claim 21, wherein, if a user authorized to access secured files classified at the new security level logs into the system, the user is granted the clearance key, together with a user key authorizing the user to access the secured files, and secured files classified at the new security level can be accessed by the user.

24. The computer-readable storage medium according to claim 23, wherein the clearance key is a private key in a pair of a public key and the private key, and the secured files are classified at the new security level with the public key.

25. The computer-readable storage medium according to claim 23, wherein, if the user is authorized to access the ith security level in the N security levels, the user is granted a second user key and a second clearance key such that the contents in the secured files classified at the (i+1)th security level and below can be accessed by the user.

26. The computer-readable storage medium according to claim 25, wherein the first key determines if the user is authorized to access the secured files classified at one of the N security levels or one of the (N+1) security levels, and the second key is in accordance with the one of the N security levels or the one of the (N+1) security levels.

27. A tangible computer-readable storage medium having stored thereon instructions that, if executed by a computing device, cause the computing device to perform a method comprising:

upon receiving a request to remove an ith security level out of the N security levels, determining if an (i−1)th security level is a 1st security level or if an (i+1)th security level is an Nth security level, wherein the 1st security level is most restrictive and the Nth security level is least restrictive among the N security levels;

if the (i−1)th security level is not the 1st security level and the (i+1)th security level is not the Nth security level, merging the ith security level with either the (i−1)th security level or the (i+1)th security level such that there are (N−1) security levels in the system,

wherein each of the secured files includes an encrypted data portion and a security portion that controls restrictive access to the encrypted data portion, the security portion including a file key encrypted by at least a first key and a second key and further protected by a set of rules, and

wherein both of the first key and the second key must be obtained by a user whose access privilege is satisfied by the rules before the contents of each of the secured files can be accessed.

28. The computer-readable storage medium according to claim 27, wherein users authorized to access secured files classified at the ith security level can access secured files classified at the (i−1)th security level if the ith security level has been merged with the (i−1)th security level.

29. The computer-readable storage medium according to claim 27, wherein users authorized to access secured files classified at the ith security level can access secured files classified at the (i+1)th security level if the ith security level has been merged with the (i+1)th security level.

30. The computer-readable storage medium according to claim 27, wherein at least two keys are needed to access secured files classified at the ith security level, and after the ith security level has been merged with the (i−1)th or (i+1)th security level, the at lest two keys are incorporated into the (i−1)th or (i+1)th security level such that users authorized to access the secured files classified at the ith security level can access the secured files.

31. The computer-readable storage medium according to claim 30, wherein the users can access secured files classified at the (i−1)th or (i+1)th security level.

32. The computer-readable storage medium according to claim 30, wherein the at least two keys include a first key associated with a designated group of users and a second key being a clearance key in accordance with the ith security level.

33. The computer-readable storage medium according to claim 32, wherein, if the user logs into the system, the user is granted the at least two keys.

34. The computer-readable storage medium according to claim 27, further comprising computer code for: if the (i−1)th security level is the 1st security level, denying the request to remove the ith security level out of the N security levels; or always folding down the ith security level with (i−1)th security level.

35. The computer-readable storage medium according to claim 27 further comprising computer code for: if the (i−1)th security level is the N security level, denying the request to remove the ith security level out of the N security levels; or always folding up the ith security level with (i−1)th security level.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : RE41,546 E
APPLICATION NO. : 11/797367
DATED : August 17, 2010
INVENTOR(S) : Klimenty Vainstein

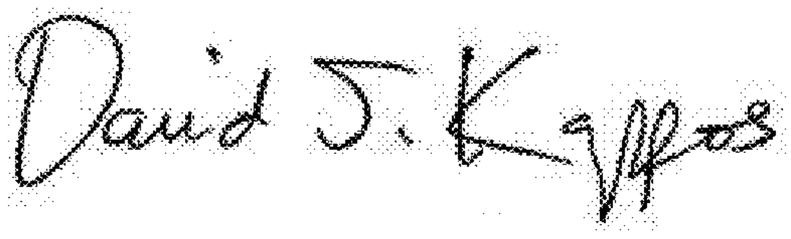
It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Title Page, Item (76), Inventor; replace "Klimenty Vainstein, 239 Shipley St. #101, San Francisco, CA (US) 94107" with --Klimenty Vainstein, Cupertino, CA (US)--.

Column 16, line 34, replace "the at lest two keys" with --the at least two keys--.

Column 19, line 18, replace "the at lest two keys" with --the at least two keys--.

Signed and Sealed this
Nineteenth Day of April, 2011



David J. Kappos
Director of the United States Patent and Trademark Office