

US00RE45348E

(19) United States

(12) Reissued Patent

Fiatal et al.

(10) Patent Number:

US RE45,348 E

(45) Date of Reissued Patent:

*Jan. 20, 2015

(54) METHOD AND APPARATUS FOR INTERCEPTING EVENTS IN A COMMUNICATION SYSTEM

(75) Inventors: Trevor A. Fiatal, Fremont, CA (US);

Jay Sutaria, Los Altos Hills, CA (US); Sridhar Nanjundeswaran, Palo Alto, CA (US); Shailesh Bayadekar,

Fremont, CA (US)

(73) Assignee: Seven Networks, Inc., San Carlos, CA

(US)

(*) Notice: This patent is subject to a terminal dis-

claimer.

(21) Appl. No.: 13/423,112

(22) Filed: Mar. 16, 2012

(Under 37 CFR 1.47)

Related U.S. Patent Documents

Reissue of:

(64) Patent No.: 7,680,281
Issued: Mar. 16, 2010
Appl. No.: 12/211,790
Filed: Sep. 16, 2008

U.S. Applications:

- (63) Continuation of application No. 11/255,291, filed on Oct. 20, 2005, now Pat. No. 7,441,271.
- (60) Provisional application No. 60/620,889, filed on Oct. 20, 2004.
- (51) Int. Cl. H04L 29/06

(2006.01)

(52) **U.S. Cl.**

(58) Field of Classification Search

USPC 380/255; 726/22; 705/14.23; 713/150 See application file for complete search history.

(56) References Cited

U.S. PATENT DOCUMENTS

222,458 A 12/1879 Connolly et al. 447,918 A 3/1891 Strowger 4,200,770 A 4/1980 Hellman et al. 4,255,796 A 3/1981 Gabbe et al. (Continued)

FOREIGN PATENT DOCUMENTS

EP 0772327 A2 5/1997 EP 1278390 A1 1/2003 (Continued)

OTHER PUBLICATIONS

Allchin, James Edward, "An Architecture for Reliable Decentralized Systems," Ph.D. Thesis, Georgia Institute of Technology, 185 pages, Sep. 1983.

(Continued)

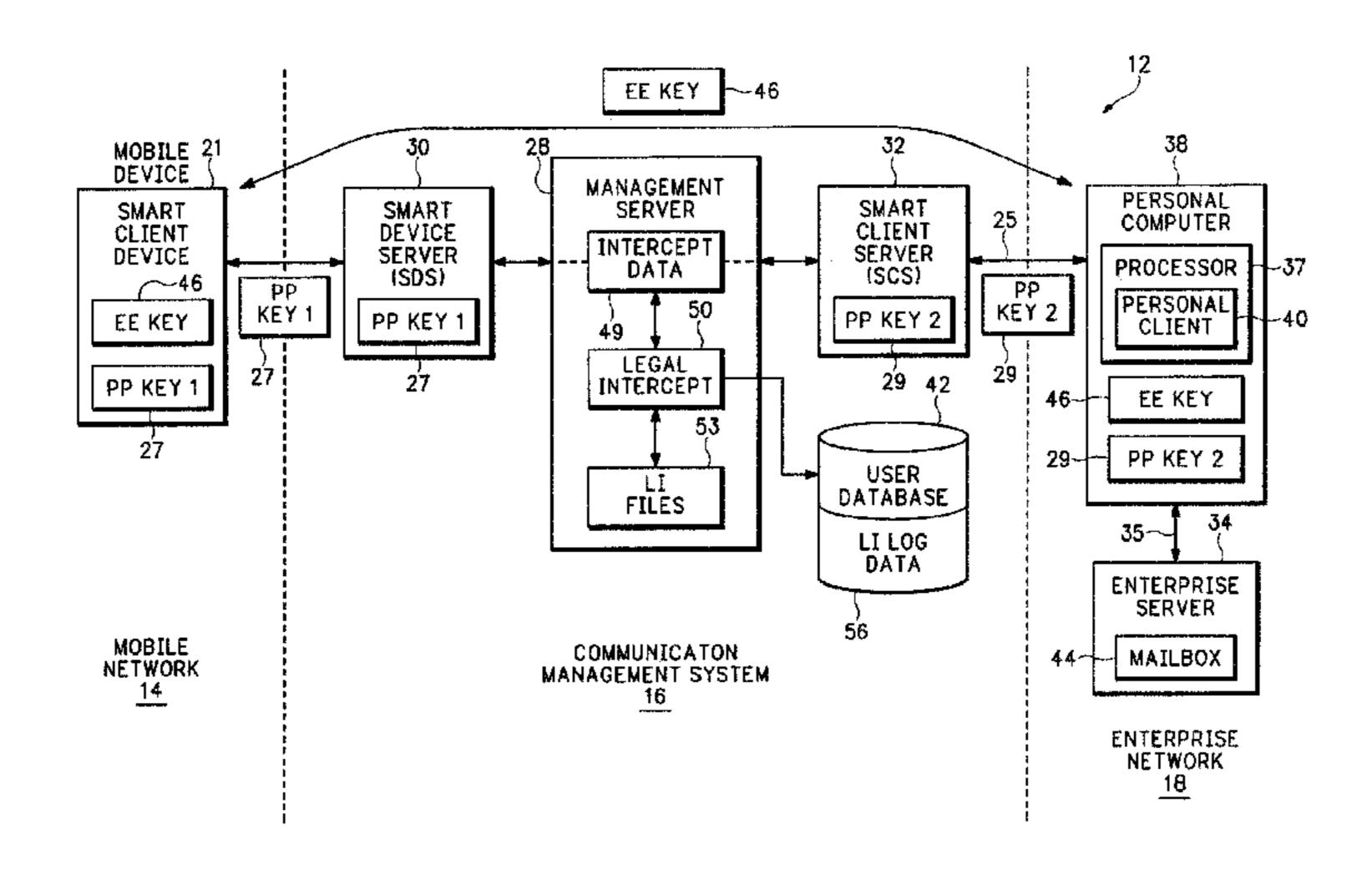
Primary Examiner — Ali Abyaneh

(74) Attorney, Agent, or Firm — NKK Patent Law, PLLC

(57) ABSTRACT

An intercept system provides more effective and more efficient compliance with legal intercept warrants. The intercept system can provide any combination of operations that include near-real-time intercept, capture of intercepted data in structured authenticated form, clear text intercept for communications where there is access to encryption keys, cipher text intercept for communications where there is no access to encryption keys, provision of transactional logs to the authorized agency, interception without altering the operation of the target services, and encryption of stored intercepted information.

45 Claims, 6 Drawing Sheets



(56)		Referen	ces Cited	5,754,938			Herz et al.
	II C	DATENIT	DOCUMENTS	5,757,916 5,758,088			MacDoran et al. Bezaire et al.
	U.S.	PAIENI	DOCUMENTS	5,758,150			Bell et al.
4,276,59	97 A	6/1981	Dissly et al.	5,758,322			Rongley
4,531,0			Wechselberger et al.	5,758,354			Huang et al.
4,807,1		2/1989	•	5,758,355			Buchanan
4,831,5	82 A		Miller et al.	5,765,171			Gehani et al.
4,875,1			Cary et al.	5,778,346			Frid-Neilsen et al.
4,897,73			Chang et al.	5,778,361 5,781,614			Nanjo et al. Brunson
, ,			O'Sullivan	5,781,901			
5,008,8 5,159,6		4/1991 10/1992	•	5,781,906			Aggarwal et al.
, ,		6/1993		5,787,430	\mathbf{A}		Doeringer et al.
·		11/1993	-	5,787,441			Beckhardt
5,283,8	56 A	2/1994	Gross et al.	5,790,425		8/1998	<u> </u>
5,357,43			Nakada et al.	5,790,790			Smith et al.
, ,		1/1995		5,790,974 5,793,413			Tognazzini Hylton et al.
5,386,56 5,392,39			Shearer et al. Crozier	5,794,210			Goldhaber et al.
5,392,3 5,434,9			Shaheen et al.	5,799,318			Cardinal et al.
5,436,9			Campana, Jr. et al.	5,802,312			Lazaridis et al.
5,438,6			Campana, Jr. et al.	5,802,454			Goshay et al.
5,479,4	72 A		Campana, Jr. et al.	5,802,518			Karaev et al.
5,487,10		1/1996		5,802,524 5,806,074			Flowers et al. Souder et al.
5,491,70			Barnaby et al.	5,800,074			Shaw et al.
5,493,69 5,519,69			Theimer et al. Frid-Nielsen et al.	·			Rossmann
5,555,3			Theimer et al.	5,818,437			Grover et al.
5,559,8			Mousseau et al.	5,819,172			Campana, Jr. et al.
5,572,5	71 A	11/1996		5,819,274			Jackson, Jr.
, ,		11/1996		5,819,284			Farber et al.
5,574,8		11/1996		5,822,324 5,822,747			Kostresti et al. Graefe et al.
, ,			Hossain et al.	5,826,269		10/1998	
5,600,83 5,603,0			Howard Theimer et al.	5,831,664			Wharton et al.
5,604,7		2/1997		5,832,483	\mathbf{A}	11/1998	Barker
, ,			Hoffman et al.	5,832,489			
5,619,50	07 A	4/1997	Tsuda	5,832,500			Burrows
5,619,6			Canale et al.	, ,			Herz et al.
5,623,60		4/1997		5,838,252		11/1998	Bradshaw et al. Kikinis
5,625,6° 5,625,8			Campana, Jr. et al. Maier et al.	5,838,768			Sumar et al.
5,627,6			Connors et al.	5,838,973			Carpenter-Smith et al.
5,630,0			Rybicki et al.	5,845,278			Kirsch et al.
5,631,9			Campana, Jr. et al.	5,852,775		12/1998	
5,632,0		5/1997		5,852,820			Burrows Wright In at al
5,634,0			Noble et al.	5,857,201 5,862,223			Wright, Jr. et al. Walker et al.
5,647,00 5,652,83			Brunson Palevich	5,867,665			Butman et al.
5,652,8 5,664,2			Crumpler et al.	5,867,817			Catallo et al.
5,666,5			Clark et al.	5,870,759	\mathbf{A}	2/1999	Bauer et al.
5,666,5		9/1997		5,884,323			Hawkins et al.
5,680,5			Mulchandani et al.	5,889,845			Staples et al.
5,682,5			Freund et al.	5,890,147 5,892,909			Peltonen et al. Grasso et al.
5,684,95 5,689,65			•	5,898,780			Liu et al.
, ,			Kikinis et al. Brankley et al.	5,898,917			Batni et al.
5,696,96		12/1997	•	5,903,723	A	5/1999	Beck et al.
5,701,4		12/1997	_	5,907,618			Gennaro et al 380/286
5,701,4			Brandli et al.	5,909,689			Van Ryzin
5,704,0			Wright, Jr.	5,913,032 5,924,096			Schwartz et al. Draper et al.
5,706,2 5,706,50			Beletic et al.	5,928,325			Shaughnessy et al.
5,706,50			Foley et al. Schloss	5,928,329			Clark et al.
5,710,9			Lagarde et al.	5,937,161	A	8/1999	Mulligan et al.
5,713,0			Keaten	5,940,813			Hutchings
5,715,40	03 A	2/1998	Stefik	5,943,676			Boothby
5,717,9		2/1998	±	5,948,066			Whalen et al.
5,721,90			Lagarde et al.	5,951,636 5,960,394		9/1999 9/1999	Gould et al.
5,721,9 5,727,20			DeVries Kucala	5,960,394			Rasansky et al.
5,727,29			Kucaia Kostreski et al.	5,961,590			Mendez et al.
5,729,7			Stone et al.	5,963,642			Goldstein
5,729,7			Meyering	5,964,833		10/1999	
5,742,9			Pepe et al.	5,968,131			Mendez et al.
5,745,3		4/1998	Leone et al.	5,974,238			Chase, Jr.
5,752,1			Malackowski et al.	5,974,327			Agrawal et al.
5,752,2	46 A	5/1998	Rogers et al.	5,978,837	A	11/1999	Foladare et al.

(56)	Referer	ices Cited	6,263,340 B1	7/2001	
119	S PATENT	DOCUMENTS	, ,		Robertson Flanagin et al.
O.,	J. 1711L/11	DOCOMILIVIS	•		Beyda et al.
5,978,933 A	11/1999	Wyld et al.	, ,		Bates et al.
, ,		O'Neil et al.	, ,		Kramer 713/172
, , , ,		Hawkins et al.	6,289,212 B1 6,289,214 B1		Stein et al. Backstrom
6,003,070 A 6,006,274 A		Frantz Hawkins et al.	, , , , , , , , , , , , , , , , , , ,		Broomhall et al.
6,016,478 A		Zhang et al.	•	9/2001	Bodnar et al.
6,016,520 A		Facq et al.			Kanevsky
6,018,762 A		Brunson et al.	6,304,881 B1 6,308,201 B1		Pivowar et al.
6,023,700 A 6,023,708 A		Owens et al. Mendez et al.	6,317,594 B1		
6,029,238 A		Furukawa	6,320,943 B1		
6,034,621 A		Kaufman	6,324,541 B1		
6,035,104 A		Zahariev	6,324,542 B1 6,324,544 B1		
6,044,372 A 6,044,381 A		Rothfus et al. Mendez et al.	6,324,587 B1		
6,047,051 A		Ginzboorog et al.	· · ·	12/2001	
6,047,327 A		Tso et al.	, ,		Massarani
6,052,563 A		Macko	6,336,138 B1 6,351,767 B1		Caswell et al. Batchelder et al.
6,052,735 A 6,057,855 A		Ulrich et al. Barkans	6,356,937 B1		Montville et al.
6,065,055 A		Hughes et al.	6,363,051 B1		Eslambolchi et al.
6,073,138 A		de l'Etraz et al.	6,363,352 B1		Dailey et al.
6,073,142 A		Geiger et al.	6,370,566 B2 6,377,810 B1		Discolo et al. Geiger et al.
6,073,165 A		Narasimhan et al. Beckhardt et al.	6,380,959 B1		Wang et al.
6,085,166 A 6,085,192 A		Mendez et al.	6,389,422 B1		Doi et al.
6,088,677 A		Spurgeon	6,389,455 B1	5/2002	
6,101,320 A	8/2000	Schuetze et al.	6,389,457 B2		Lazaridis et al.
6,101,480 A		Conmy et al.	6,397,057 B1 6,397,230 B1		Malackowski et al. Carmel et al.
6,101,531 A 6,112,181 A		Eggleston et al. Shear et al.	6,401,104 B1		LaRue et al.
6,119,014 A		Alperovich et al.	6,401,112 B1		Boyer et al.
6,119,171 A		Alkhatib	6,401,113 B2		Lazaridis et al.
6,125,369 A		Wu et al.	6,405,197 B2 6,411,696 B1		Gilmour Iverson et al.
6,125,388 A 6,128,627 A		Reisman Mattis et al.			Colligan et al.
6,130,898 A		Kostreski et al.	6,418,308 B1	7/2002	Heinonen et al.
6,131,096 A	10/2000	Ng et al.	6,421,669 B1		Gilmour et al.
6,131,116 A		Riggins et al.	6,421,781 B1 6,430,602 B1		Fox et al. Kay et al.
6,134,432 A 6,138,013 A		Holmes et al. Blanchard et al 455/428	C 420 505 D2		Mousseau et al.
6,138,124 A		Beckhardt	6,438,612 B1		Ylonen et al.
6,138,128 A		Perkowitz et al.	, ,		Takahashi et al.
6,138,146 A		Moon et al.	6,442,637 B1 6,446,118 B1		Hawkins et al. Gottlieb
6,141,664 A 6,151,606 A		Boothby Mendez	, ,		Godfrey et al.
6,157,630 A			6,463,464 B1		
6,161,140 A			6,487,557 B1 6,487,560 B1		Nagatomo La Rue et al
6,167,379 A 6,167,435 A		Dean et al. Druckenmiller et al.	6,490,353 B1		
6,170,014 B1		Darago et al.	6,496,802 B1		
6,173,312 B1	1/2001	Atarashi et al.	·		Hesselink et al.
6,173,446 B1		Khan et al.	6,505,214 B1 6,516,327 B1		Sherman et al. Zondervan et al.
6,175,831 B1 6,178,419 B1		Weinreich et al. Legh-Smith et al.	, ,		Chang et al.
6,181,935 B1		Gossman et al.	6,526,506 B1	2/2003	
6,185,184 B1	2/2001	Mattaway et al.	6,529,908 B1		Piett et al.
6,195,533 B1		Tkatch et al.	6,532,446 B1 6,535,892 B1	3/2003 3/2003	LaRue et al.
6,198,696 B1 6,198,922 B1		Korpi et al. Baynham	6,546,005 B1		Berkley et al.
6,201,469 B1		Balch et al.	6,549,939 B1		Ford et al.
6,202,085 B1		Benson et al.	6,556,217 B1		Mäkipää et al.
6,205,448 B1		Kruglikov et al.	6,593,944 B1 6,601,026 B2		Nicolas et al. Appelt et al.
6,212,529 B1 6,219,694 B1		Boothby et al. Lazaridis et al.	6,615,253 B1		Bowman-Amuah
6,221,877 B1		Aronov et al.	6,618,710 B1		Zondervan et al.
6,223,187 B1		Boothby et al.	6,621,892 B1		Banister et al.
6,226,686 B1		Rothschild et al.	6,625,621 B2 6,636,482 B2		Tan et al. Cloonan et al.
6,233,341 B1 6,243,705 B1		Riggins Kucala			Ejiri et al.
6,246,875 B1		Seazholtz et al.			Corrigan et al.
6,247,135 B1	6/2001	Feague	6,640,244 B1	10/2003	Bowman-Amuah
6,249,808 B1		Seshadri	, ,		Bowman-Amuah
6,256,666 B1		Singhal Hashimoto et al	6,643,650 B1 6,643,688 B1		
0,203,201 B1	//ZUU1	Hashimoto et al.	6,643,688 B1	11/2003	1 U15Z

(56)		Referen	ces Cited	6,970,879 B1 6,972,682 B2		Gilmour Lareau et al.
	U.S.	PATENT	DOCUMENTS	6,973,299 B2	12/2005	
				6,981,041 B2		Araujo et al.
	6,647,384 B2	11/2003	Gilmour	6,981,047 B2		Hanson et al.
	, ,		Irlam et al.	6,985,933 B1 6,985,983 B2		Singhal et al. Pellegrino et al.
	/ /	12/2003	Buckham et al.	6,986,061 B1		Kunzinger
	, ,		McFadden	6,987,734 B2		Hundemer
	/ /		Creemer et al.	6,990,472 B2		Rosenhaft et al.
			Kruglikov et al.	6,993,326 B2		Link, II et al.
	6,671,757 B1			6,993,327 B2 6,996,627 B1		Mathis Carden
	6,694,336 B1 6,697,807 B2		Multer et al. McGeachie	6,999,753 B2		Beckmann et al.
	6,701,378 B1		Gilhuly et al.	7,020,685 B1		Chen et al.
	6,707,801 B2	3/2004		7,024,491 B1		Hanmann et al.
	6,708,221 B1		Mendez et al.	7,026,984 B1 7,032,242 B1		Thandu et al. Grabelsky et al.
	6,714,965 B2 6,721,787 B1		Kakuta et al. Hiscock	7,035,630 B2		Knowles
	6,727,917 B1		Chew et al.	7,046,993 B2		Haaramo et al.
	6,728,530 B1		Heinonen et al.	7,047,202 B2		Jaipuria et al.
	6,728,786 B2		Hawkins et al.	7,062,024 B2 7,069,308 B2		Kreckel et al. Abrams
	6,732,101 B1 6,732,158 B1	5/2004 5/2004	Hesselink et al.	7,072,678 B2		Allison
	6,735,591 B2	5/2004		7,079,499 B1		Akhtar et al.
	6,741,232 B1		Siedlikowski et al.	7,080,371 B1		Arnaiz et al.
	6,741,855 B1		Martin et al.	7,082,316 B2 7,085,365 B2		Eiden et al. Kauppinen
	6,742,015 B1 6,742,059 B1		Bowman-Amuah Todd et al.	7,096,030 B2		Huomo
	6,745,024 B1		DeJaco et al.	7,100,821 B2	9/2006	
	6,745,326 B1	6/2004		7,103,432 B2		Drader et al.
	6,756,882 B2		Benes et al.	7,120,692 B2 7,120,928 B2		Hesselink et al. Sheth et al.
	6,757,362 B1 6,757,696 B2		Cooper et al. Multer et al.	7,120,928 B2 7,130,839 B2		Boreham et al.
	6,757,090 B2		Craig et al.	7,136,645 B2		Hanson et al.
	6,760,916 B2		Holtz et al.	7,139,555 B2	11/2006	<u> </u>
	6,771,294 B1		Pulli et al.	7,139,565 B2		Fiatal et al.
	6,775,362 B1		Ransom Mougganu et el	7,140,549 B2 7,146,645 B1		Hellsten et al.
	6,779,019 B1 6,782,409 B1		Mousseau et al. Yoshida	7,149,780 B2		Quine et al.
	6,785,868 B1	8/2004		7,149,789 B2		Slivka et al.
	6,785,906 B1		Gaughan et al.	7,149,959 B1		Jones et al.
	6,799,190 B1		Boothby	7,162,241 B2 7,165,727 B2		Kim et al. de Jong
	6,804,707 B1 6,816,849 B1	10/2004	Ronning Halt Ir	7,172,118 B2	2/2007	•
	6,820,088 B1		Hind et al.	7,181,228 B2		Boesch
	6,820,204 B1		Desai et al.	7,184,790 B2		Dorenbosch et al.
	6,829,487 B2		Eiden et al.	7,185,362 B2 7,194,273 B2		Hawkes et al. Vaudreuil
	6,834,195 B2 6,847,974 B2		Brandenberg et al. Wachtel	7,200,390 B1		Henager et al.
	6,850,757 B2		Watanabe et al.	7,203,733 B1	4/2007	
	6,859,212 B2		Kumar et al.	7,206,806 B2 7,209,757 B2	4/2007	
	6,859,440 B1		Sonti et al.	7,209,737 B2 7,210,121 B2		Naghian et al. Xia et al.
	6,867,774 B1 6,868,447 B1		Halmshaw et al. Slaughter et al.	7,219,139 B2		Martin et al.
	6,871,220 B1		Rajan et al.	7,219,222 B1		Durbin et al.
	6,871,236 B2		Fishman et al.	7,224,957 B2 7,231,206 B2		Spector Cudak et al.
	6,873,688 B1 6,874,017 B1		Aarnio Inque et el	7,231,200 B2 7,233,795 B1	6/2007	
	6,879,985 B2		Inoue et al. Deguchi et al.	7,234,111 B2		Chu et al.
	6,886,030 B1		Easterbrook et al.	7,239,877 B2		Corneille et al.
	6,892,070 B2		Warrier et al.	7,240,095 B1 7,242,680 B2	7/2007	Lewis Gallant
	6,892,196 B1		Hughes Vramor et al	7,242,080 B2 7,245,926 B2		Liao et al.
	6,895,394 B1 6,895,558 B1		Kremer et al. Loveland	7,257,391 B2		Burgess et al.
	6,898,427 B1		Griffith et al.	7,257,639 B1		Li et al.
	6,922,547 B2		O'Neill et al.	7,259,666 B1		Hermsmeyer et al. Riera Jorba et al.
	6,922,721 B1		Minborg et al.	7,260,552 B2 7,260,590 B1		Williams
	6,925,477 B1 6,931,529 B2		Champagne et al. Kunzinger	7,260,651 B2		Parrella, Sr. et al.
	6,938,079 B1		Anderson et al.	7,272,830 B2		de Jong
	6,944,447 B2		Portman et al.	7,277,408 B2	10/2007	
	6,944,662 B2		Devine et al.	7,284,664 B1		Ivchenko et al.
	6,947,770 B2 6,950,862 B1*		Rydbeck Puthiyandyil et al 709/220	7,289,792 B1 7,289,964 B1		Turunen Bowman-Amuah
	6,957,397 B1		Hawkins et al.	7,289,904 B1 7,289,971 B1		O'Neil et al.
	, ,		Aloni et al.	7,293,107 B1		Hanson et al.
	6,966,058 B2			7,295,853 B2		
	6,968,175 B2	11/2005	Raivisto et al.	7,296,155 B1	11/2007	Trostle et al.

(56)	Referen	ices Cited	7,917,468 B2		Ariel et al.
115	PATENT	DOCUMENTS	7,917,303 B2 7,921,167 B2		van Gent et al. Shroff et al.
0.0	, 17X1L/1V1	DOCOMILIVIS	7,930,416 B2		Miller et al.
7,305,252 B2	12/2007	Britt et al.	7,933,929 B1		McClendon et al.
, ,		Boynton et al.	7,937,091 B2		Roman et al.
7,310,350 B1	12/2007	Shao et al.	7,970,860 B2		Kline et al.
7,310,729 B2		Gordon et al.	7,996,487 B2 8,005,891 B2		Snyder Knowles et al.
7,324,473 B2		Corneille et al.			Sutaria et al.
7,349,871 B2 7,353,274 B1		Labrou et al. Rouhi et al.	8,032,409 B1		Mikurak
, ,		Hartmaier et al.	, , , , , , , , , , , , , , , , , , ,		Sutaria et al.
7,373,386 B2		Gardner et al.	8,069,166 B2		Alvarado et al.
7,374,099 B2		de Jong	8,078,158 B2		
7,376,701 B2		Bhargava et al.	8,107,921 B2 8,116,214 B2		Backholm et al.
7,382,879 B1		Miller	8,110,214 B2 8,127,342 B2		Boynton et al.
7,388,950 B2 7,389,412 B2		Elsey et al. Sharma et al.	8,166,164 B1		Luna et al.
7,392,483 B2		Wong et al.	8,190,701 B2		Luna et al.
7,395,329 B1		Holt et al.	8,194,680 B1		Brandwine et al.
7,398,271 B1		Borkovsky et al.	8,204,953 B2		Luna et al.
7,430,609 B2		Brown et al.	8,209,709 B2 8,260,852 B1		Fleming Cselle
7,441,271 B2 7,443,847 B1		Fiatal et al. Albert et al.	8,549,587 B2		Boynton et al.
, ,		Fitzpatrick et al.	2001/0009025 A		Ahonen
7,465,231 B2		Lewin et al.	2001/0010046 A		Muyres et al.
7,469,125 B2		Nurmi	2001/0013069 A		
7,483,036 B2			2001/0023414 AI		Kumar et al. Smith et al.
7,499,537 B2		Elsey et al.	2001/0029524 AI 2001/0032254 AI		Hawkins et al.
7,502,615 B2 7,519,042 B2		Wilhoite et al. Gorday et al.	2001/0032251 AI		
7,532,571 B1		Price et al.	2001/0034244 A		±
7,539,665 B2		Mendez			Mitty et al 713/168
7,539,728 B2	5/2009	Perepa et al.	2001/0039191 A1		
7,548,947 B2		Karsriel et al.	2001/0041566 AI 2001/0042009 AI		
7,548,969 B2		Tripp et al.	2001/0042009 A1 2001/0042099 A1		•
7,551,900 B2 7,567,575 B2		Kang et al. Chen et al.	2001/0043148 A		
7,574,208 B2		Hanson et al.	2001/0052052 A	1 12/2001	Peng
7,575,171 B2			2001/0053687 A		
7,584,294 B2			2002/0002478 AI 2002/0002591 AI		Swart et al. Ketola
7,587,482 B2		Henderson et al.	2002/0002391 A1 2002/0007303 A1		Brookler et al.
7,587,608 B2 7,593,714 B2		Haller et al. Schultz et al.	2002/0013727 A		
7,596,608 B2		Alexander et al.	2002/0019225 A		Miyashita
7,596,791 B2			2002/0019812 AI		Board et al.
7,613,792 B2			2002/0035556 AI 2002/0035617 AI		Shah et al. Lynch et al.
7,630,986 B1 7,634,558 B1		Herz et al. Mangal et al	2002/0033017 AT		Seaman et al.
		Backholm et al.	2002/0042875 A		Shukla
, ,		Appelman et al.	2002/0049818 A		Gilhuly et al.
7,650,416 B2	1/2010	Wu et al.	2002/0049828 A1		
7,672,291 B2		•	2002/0053078 AI 2002/0055351 AI		Holtz et al. Elsey et al.
7,672,439 B2		Appelman et al.	2002/0059331 A1 2002/0059201 A1		
7,680,281 B2 7,684,346 B2		Fiatal et al. Valli	2002/0059457 A		Ballard et al.
7,689,664 B2		Karlberg	2002/0068559 A		Sharma et al.
7,693,555 B2		Srinivasan et al.	2002/0073207 A		Widger et al.
7,693,944 B2		Appelman et al.	2002/0077077 A1		Rezvani et al.
7,694,008 B2		Chang et al.	2002/0077084 AI 2002/0078384 AI		Zellner et al. Hippelainen
7,706,781 B2 7,707,573 B1		Backholm et al. Marmaros et al.	2002/0070504 AI 2002/0087549 AI		Mostafa
7,752,633 B1		Fleming	2002/0087679 A		Pulley et al.
7,757,956 B2		Koenck et al.	2002/0087883 A		Wohlgemuth et al.
7,769,395 B2		Fiatal et al.	2002/0089542 A		Imamura
/ /		Backholm et al.	2002/0091921 AI 2002/0095319 AI		Kunzinger Swart et al.
7,769,805 B1		Barnes et al.	2002/0095319 A1 2002/0095328 A1		Swart et al.
7,778,792 B2 7,783,757 B2		Huang et al. Plamondon	2002/0095320 A1		Swart et al.
7,796,742 B1		Sutaria et al.	2002/0095399 A		Devine et al.
7,797,064 B2	9/2010	Loomis et al.	2002/0098855 Al		Hartmaier et al.
7,809,818 B2		Plamondon	2002/0099613 A		Swart et al.
7,827,055 B1		Snodgrass et al.	2002/0099809 AI		
7,827,597 B2		Boynton et al.	2002/0101975 AI 2002/0103934 AI		Tiburtius et al. Fishman et al.
7,853,563 B2 7,877,703 B1		Alvarado et al. Elemino	2002/0103934 AI 2002/0107944 AI		Bai et al.
7,881,745 B1		•	2002/0107944 A1 2002/0107985 A1		Hwang et al.
7,899,996 B1		Levin-Michael	2002/0116499 A		Ennus et al.
7,908,656 B1	3/2011	Mu	2002/0116501 A	1 8/2002	Ho et al.

(56)	Referer	ices Cited	2003/0236857 A1		Takase et al.
	U.S. PATENT	DOCUMENTS	2003/0236981 A1 2004/0002324 A1		Marmigere et al. Juntunen et al.
			2004/0006630 A1		Friend et al.
2002/0120388		Bullock	2004/0015504 A1 2004/0024795 A1		Ahad et al. Hind et al.
2002/0120766 2002/0120779		Okajima et al. Teeple et al.	2004/0024733 AT		Ferguson et al.
2002/0126701		Requena	2004/0024892 A1	2/2004	Creswell et al.
2002/0133504		Vlahos et al.	2004/0027326 A1		Hays et al.
2002/0144109		Benantar et al.	2004/0027375 A1 2004/0027378 A1		Ellis et al. Hays et al.
2002/0146129 2002/0152379		Kapian Gefwert et al.	2004/0043770 A1		Amit et al.
2002/0155848		Suryanarayana	2004/0049579 A1		Ims et al.
2002/0156839		Peterson et al.	2004/0049599 A1 2004/0051715 A1		Friend et al. Brokenshire et al.
2002/0158908 2002/0161587		Vaajala et al. Pitts, III et al.	2004/0051713 A1 2004/0054719 A1		Daigle et al.
2002/0101907		Munger et al.	2004/0054739 A1	3/2004	Friend et al.
2002/0161928			2004/0064445 A1 2004/0064488 A1		Pfleging et al.
2002/0164977 2002/0167484		Link, II et al. Hatanaka et al.	2004/0004488 A1 2004/0068579 A1	4/2004 4/2004	Marmigere et al.
2002/0107484			2004/0068698 A1		Wu et al.
2002/0186848			2004/0073476 A1		Donahue et al.
2002/0188940		Breckner et al.	2004/0073651 A1 2004/0075675 A1		Beaulieu et al. Raivisto et al.
2002/0193094 2002/0194209		Lawless et al. Bolosky et al.	2004/0075695 A1		Chew et al.
2002/0198027		Rydbeck	2004/0078814 A1	4/2004	
2003/0005151		Ullman et al.	2004/0080515 A1 2004/0082346 A1		Hagiwara Skytt et al.
2003/0014491 2003/0022662		Horvitz et al. Mittal	2004/0082546 A1		Lagadec et al.
2003/0022002		Moroo	2004/0103147 A1		Flesher et al.
2003/0023975	A1 1/2003	Schrader et al.	2004/0107319 A1		D'Orto et al.
2003/0028430		Zimmerman Paranaga et el	2004/0110497 A1 2004/0120323 A1	6/2004 6/2004	Viikari et al.
2003/0028441 2003/0046433		Barsness et al. Luzzatti et al.	2004/0123095 A1		Marshall
2003/0046586		Bheemarasetti et al.	2004/0123304 A1		Black et al.
2003/0046587		Bheemarasetti et al.	2004/0127214 A1 2004/0128375 A1		Reddy et al. Rockwell
2003/0050041 2003/0054810		wu Chen et al.	2004/0120373 AT		Herrero et al.
2003/0056096		Albert et al.	2004/0141011 A1		Smethers et al.
2003/0060188		Gidron et al.	2004/0147248 A1 2004/0147262 A1	7/2004	Will Lescuyer et al.
2003/0063120 2003/0065738		Wong et al. Yang et al.	2004/0147202 A1 2004/0148375 A1		Levett et al.
2003/0005738		Shnier	2004/0158611 A1	8/2004	Daniell et al.
2003/0065802		Vitikainen et al.	2004/0167966 A1		Lee et al.
2003/0070061		Wong et al. Dimental et al.	2004/0170257 A1 2004/0172481 A1		Gross et al. Engstrom
2003/0072451 2003/0078880		Pimentel et al. Alley et al.	2004/0176128 A1		Grabelsky et al.
2003/0084165	A1 5/2003	Kjellberg et al.	2004/0177369 A1		Akins, III
2003/0088629		Berkowitz et al.	2004/0179513 A1 2004/0181550 A1		Smith et al 370/352 Warsta et al.
2003/0093691 2003/0097381		Simon et al. Detweiler et al.	2004/0184475 A1	9/2004	
2003/0100321		Rao et al.	2004/0186902 A1		Stewart
2003/0100326		Grube et al.	2004/0189610 A1 2004/0199497 A1	9/2004 10/2004	Friend Timmons
2003/0117432 2003/0120685		Kautto-Kiovula et al. Duncombe et al.			Kucharewski et al.
2003/0125023		Fishler	2004/0199663 A1		Horvitz et al.
2003/0126216		Avila et al.	2004/0205248 A1 2004/0205330 A1		Little et al. Godfrey et al.
2003/0130984 2003/0145038		Quinlan et al. Bin Tariq et al.			Joyce et al.
2003/0146934		Bailey et al.	2004/0210639 A1	10/2004	Ben-Yoseph et al.
2003/0153338		Herz et al.			Kong et al. Blanco et al.
2003/0154212 2003/0156146		Schirmer et al. Suomela et al.			Colby, Jr.
2003/0150140		Fiatal et al.	2004/0236792 A1	11/2004	Celik
2003/0169262	A1 9/2003	Lavelle et al.			Kruis et al.
2003/0177281		McQuillan et al. Sturniolo et al.	2004/0252816 A1 2004/0255126 A1*	12/2004 12/2004	Reith 713/183
2003/0182431 2003/0187984		Banavar et al.			Elsey et al.
2003/0204605		Hudson et al.			Elsey et al.
2003/0208529		Pendyala et al.		12/2004	Ackley Miyata et al.
2003/0208559 2003/0210666		Velline et al. Trossen et al.			Ginzburg et al.
2003/0210808		Lohtia et al.	2004/0266364 A1		Nguyen et al.
2003/0217098		Bobde et al.	2004/0268148 A1		Karjala et al.
2003/0217142		Bobde et al.	2005/0002501 A1		Elsey et al.
2003/0223554 2003/0227487			2005/0002508 A1 2005/0002509 A1		Elsey et al. Elsey et al.
	A1 12/2003	2	2005/0002510 A1		•
2003/0235308	A1 12/2003	Boynton et al.	2005/0010694 A1	1/2005	Ma et al.

(56)	Referer	ices Cited	2006/0020804	A 1	1/2006	Schleifer et al.
			2006/0020947			Hallamaa et al.
U.S.	PATENT	DOCUMENTS	2006/0021023 2006/0022048			Stewart et al. Johnson
2005/0015432 A1	1/2005	Cohen	2006/0022048			Cabillic et al.
2005/0013432 A1 2005/0021750 A1		Abrams	2006/0029062		2/2006	
2005/0022000 A1		Inomata et al.	2006/0029063			Rao et al.
2005/0022182 A1		Mittal Cailor et al	2006/0029064 2006/0031114			Rao et al. Zommers
2005/0027591 A9 2005/0027716 A1		Gailey et al. Apfel	2006/0031300			Kock et al.
2005/0027710 A1		Johnson	2006/0031365			Kay et al.
2005/0033812 A1		McCarthy et al.	2006/0031428			Wikman
2005/0033926 A1		Dumont	2006/0031785 2006/0037071			Raciborski Rao et al.
2005/0037741 A1 2005/0038707 A1		Gilbert Roever et al.	2006/0046686			Hawkins et al.
2005/0038707 A1		Roever et al.	2006/0047844		3/2006	
2005/0038863 A1		Onyon et al.	2006/0048061			Forlenza et al.
2005/0041793 A1		Fulton et al.	2006/0052091 2006/0052137			Onyon et al. Randall et al.
2005/0044144 A1 2005/0055578 A1		Malik et al. Wright et al.	2006/0059495			Spector
2005/0063544 A1*		Uusitalo et al 380/277	2006/0063544			Zhao et al.
2005/0071489 A1		Parupudi et al.	2006/0069686 2006/0069687			Beyda et al. Cui et al.
2005/0071674 A1 2005/0073982 A1		Chou et al. Corneille et al.	2006/0069715			Vayssiere
2005/0075982 A1 2005/0076136 A1		Cho et al.	2006/0069742		3/2006	-
2005/0076241 A1		Appelman	2006/0069746			Davis et al.
2005/0086540 A1		Gunter et al.	2006/0073810 2006/0074951			Pyhalammi et al. Beier et al.
2005/0094625 A1 2005/0097225 A1		Bouat Glatt et al.	2006/0074931			Zager et al.
2005/0097223 A1 2005/0097570 A1		Bomers	2006/0084410			Sutaria et al.
2005/0101307 A1		Brugge et al.	2006/0085503			Stoye et al.
2005/0102257 A1		Onyon et al.	2006/0093026 2006/0093135			Montojo et al. Fiatal et al.
2005/0102328 A1 2005/0102351 A1		Ring et al. Jiang et al.	2006/0099133			Staton et al.
2005/0102551 A1 2005/0108427 A1	5/2005	_	2006/0099970			Morgan et al.
2005/0117606 A1	6/2005	•	2006/0112177			Barkley et al.
2005/0120082 A1		Hesselink et al.	2006/0123042 2006/0132495			Xie et al. Anderson
2005/0120084 A1 2005/0120181 A1		Hu et al. Arunagirinathan et al.	2006/0132493			Forbes et al.
2005/0120131 A1 2005/0122333 A1		Sumanaweera et al.	2006/0143464			Ananthanarayanan et al.
2005/0124332 A1		Clark et al.	2006/0149591			Hauf et al.
2005/0138111 A1		Aton et al.	2006/0149843 2006/0149970		7/2006	Rhoads et al. Imazu
2005/0138176 A1 2005/0144219 A1		Singh et al. Terada	2006/0155822			Yang et al.
2005/0147130 A1		Hurwitz et al.	2006/0161621			Rosenberg
2005/0154698 A1		Ikezawa et al.	2006/0165226 2006/0167969			Ernst et al. Andreev et al.
2005/0154796 A1 2005/0154836 A1		Forsyth Stoology et al	2006/0167909			Eisenberger et al.
2005/0154830 A1 2005/0155027 A1	7/2005	Steeley et al. Wei	2006/0168164			Lemson
2005/0164703 A1		Huynh	2006/0179410		8/2006	
2005/0164721 A1		Eric Yeh et al.	2006/0188864 2006/0190428		8/2006 8/2006	Shah Jung et al.
2005/0165909 A1 2005/0170776 A1		Cromer et al. Siorpaes	2006/0190569			
2005/01/07/0 A1*		Anderholm et al 726/22	2006/0190984			Heard et al.
2005/0188038 A1	8/2005	Yabe	2006/0192014			Hamilton et al.
2005/0193036 A1		Phillips et al.	2006/0195570 2006/0209842			Zellner et al. Creamer et al.
2005/0193096 A1 2005/0198170 A1		Yu et al. LaMay et al.	2006/0212531			Kikkawa et al.
2005/0203966 A1		Labrou et al.	2006/0224629		4	Alexander et al.
2005/0210104 A1		Torvinen	2006/0230394			Forth et al.
2005/0210125 A1 2005/0222891 A1	9/2005	Li Chan et al.	2006/0240804 2006/0240805			Backholm et al. Backholm et al.
2005/0222891 A1 2005/0228812 A1		Hansmann et al.	2006/0242137			Shah et al.
2005/0232295 A1			2006/0242210			Ring et al.
2005/0234860 A1		Roever et al.	2006/0242320 2006/0242607			Nettle et al.
2005/0235214 A1 2005/0246139 A1		Shimizu et al. Rivenbark et al	2006/0252435			Henderson et al.
2005/0248135 A1					11/2006	Pacholec et al.
2005/0251555 A1	11/2005	Little, II	2006/0253605			Sundarrajan et al.
2005/0254443 A1		Campbell et al.	2006/0259923 2006/0265595		11/2006 11/2006	Chiu Scottodiluzio
2005/0262220 A1 2005/0273804 A1			2006/0203393		11/2006	
2005/0278307 A1			2006/0277265			Backholm et al.
2005/0278641 A1		Mansour et al.	2006/0277271			Morse et al.
2005/0278647 A1		Leavitt et al.	2006/0294071			Weare et al.
2005/0288006 A1 2006/0012672 A1		-	2006/0294223			Glasgow et al. Alexion-Tiernan et al.
2006/0012672 A1 2006/0020525 A1		Borelli et al.	2007/0003738			Asami et al.
2006/0020525 711 2006/0020580 A1		Dettinger et al.	2007/0011367			Scott et al.

(56)		Referen	ces Cited	2008/0077571			Harris et al.
	TIC	DATENIT	DOCLIMENTS	2008/0085719 2008/0085724			Kuchibhotla et al. Cormier et al.
	0.5.	PAIENI	DOCUMENTS	2008/0085724			Dion et al.
2007/0019610	n A 1	1/2007	Backholm et al.	2008/0091773			Hameen-Anttila
2007/001901		1/2007		2008/0103877			Gerken
2007/002777			Hwang	2008/0104666	A 1	5/2008	Dillaway
2007/0027832	2 A1		Fiatal et al.	2008/0108298			Selen et al.
2007/0027880	6 A1	2/2007	Gent et al.	2008/0114881			Lee et al.
2007/002791			Ariel et al.	2008/0125225			Lazaridis et al.
2007/0027920			Alvarado et al.	2008/0130663 2008/0133326			Fridman et al. Goncalves et al.
2007/002792			Alvarado et al.	2008/0133520			Gent et al.
2007/0027930 2007/003353		2/2007 2/2007	Alvarado et al. Marsh	2008/0133708			Alvarado et al.
2007/003856			Allaire et al.	2008/0134292	A1	6/2008	Ariel et al.
2007/003893			Allaire et al.	2008/0140665			Ariel et al.
2007/004404	1 A1	2/2007	Beynon et al.	2008/0151817			Fitchett et al.
2007/004925			Thibeault	2008/0154870 2008/0155613			Evermann et al. Benya et al.
2007/0060190			Sharma	2008/0133013			Guedalia et al.
2007/0061393 2007/006714		3/2007 3/2007		2008/0167019			Guedalia et al.
2007/006714			Grant et al.	2008/0168145			Wilson
2007/0067424			Raciborski et al.	2008/0183800	A 1	7/2008	Herzog et al.
2007/007093	1 A1		Lewis et al.	2008/0192820			Brooks et al.
2007/007261			Lewis et al.	2008/0198995			McGary et al.
2007/007885			Punaganti et al.	2008/0201362 2008/0201751			Multer et al. Ahmed et al.
2007/007896			East et al.	2008/0201731			Maharajh et al.
2007/0088852 2007/010562			Levkovitz Campbell	2008/0207102			Hasek
2007/010302			Park et al.	2008/0214148			Ramer et al.
2007/011622			Burke et al.	2008/0216094	A 1		Anderson et al.
2007/0118620	0 A1	5/2007	Cartmell et al.	2008/0220797			Meiby et al.
2007/0130103			Simpson et al.	2008/0232290			Elzur et al.
2007/013021			Linyard et al.	2008/0233983 2008/0242370			Park et al. Lando et al.
2007/0140193			Dosa et al.	2008/0242370			Caron et al.
2007/014731′ 2007/014741			Smith et al. Bijwaard et al.	2008/0270379			Ramakrishna
2007/014741			Khawand et al.	2008/0273498	A1	11/2008	Jalil et al.
2007/0156824			Thompson	2008/0281798			Chatterjee et al.
2007/0156842	2 A1		Vermeulen et al.	2008/0288659			Hasha et al.
2007/0162514			Civetta et al.	2008/0298386 2008/0299956		12/2008	Bailey et al.
2007/0167173			Al-Harbi	2008/0299930			Mehta et al.
2007/0174433 2007/0175993		8/2007	Mendez et al. Lev	2008/0301300		12/2008	
2007/017355			Boyd et al.	2008/0313282	A1	12/2008	Warila et al.
2007/0220080			Humphrey	2009/0010204			Pratt, Jr. et al.
2007/0220099	9 A1	9/2007	Di Giorgio et al.	2009/0010259			Sirotkin
2007/023385:			Brown et al.	2009/0012841 2009/0016526			Saft et al. Fiatal et al.
2007/0237313			McGary	2009/0010320			Ellis et al.
2007/0245010 2007/024936:		10/2007	Arn et al. Jendbro	2009/0019532			Jacobsen et al.
2007/024930.			Milic-Frayling et al.	2009/0024794			Iyer et al.
2007/025463		11/2007		2009/0031006			Johnson
2007/0255848			Sewall et al.	2009/0052372			Durazzo et al.
2007/0264993		11/2007	\mathbf{c}	2009/0054034			Backholm et al.
2007/0267492			Maclaine Pont	2009/0055353 2009/0059950			Meema Gao et al.
2007/027692: 2007/0276926			LaJoie et al. LaJoie et al.	2009/0063647			Backholm et al.
2007/0270920			Shenfield	2009/0075683			Backholm et al.
2007/029078			Fiatal et al.	2009/0077263	A1	3/2009	Koganti et al.
2007/029320			Guedalia et al.	2009/0077326			Motohashi
2007/0293233	8 A1	12/2007	Fiatal et al.	2009/0094317			Venkitaraman
2007/029395			Stehle et al.	2009/0100416 2009/0110179			Brown et al. Elsey et al.
2007/029429:			Finkelstein et al.	2009/0110179			Fitzpatrick et al.
2007/0294763 2007/029670			Udezue et al. Pope et al.	2009/0125523			Fitzpatrick et al.
2007/0299913				2009/0144632	A1		Mendez
2008/000171		1/2008		2009/0147008			Do et al.
2008/000809:	5 A1	1/2008	Gilfix	2009/0149203			Backholm et al.
2008/000934			Graham et al.	2009/0156178			Elsey et al.
2008/0016230			Beverly et al.	2009/0157792		6/2009	_
2008/0032713		2/2008		2009/0164433 2009/0164560		6/2009 6/2009	
2008/003403 2008/003778′			Weisbrot et al. Boynton et al.	2009/0104360			Jackson et al.
2008/005778			Gerken	2009/01/2303		7/2009	
2008/0059393			Tsutsui	2009/0182500		7/2009	
2008/0061142			Howcroft et al.	2009/0187939			
2008/0068519			Adler et al.	2009/0191903	A1	7/2009	•
2008/007750	6 A1	3/2008	Rampell et al.	2009/0193130	A1	7/2009	Fiatal

(56)	Referen	ices Cited	2011/0184827 2011/0185355		2011	Hubert Chawla et al.
U.S.	PATENT	DOCUMENTS	2011/0183333			Fiatal
			2011/0191474			Fiatal
2009/0193338 A1	7/2009		2011/0201304			Sutaria et al.
2009/0215504 A1		Lando Paugael et el	2011/0207436 2011/0208810			van Gent et al. Li et al.
2009/0221326 A1 2009/0228545 A1		Roussel et al. Mendez et al.	2011/0213800			Saros et al.
2009/0241180 A1			2011/0213898			Fiatal et al.
2009/0248670 A1	10/2009		2011/0214182			Adams et al.
2009/0248696 A1 2009/0248794 A1		Rowles et al. Helms et al.	2011/0238772 2011/0246950			Fiatal Luna et al.
2009/0248/94 A1 2009/0248878 A1		Tran et al.	2011/0252088			Fiatal
		Mahany et al.	2011/0264622			Vargas et al.
2009/0254589 A1		Nair et al.	2011/0264731 2011/0294463			Knowles et al.
2009/0254971 A1 2009/0264138 A1		Herz et al. Kang et al.	2011/0294464			Fiatal
		Jeide et al.	2011/0296050			Cherukuri
		Bhatt et al.	2011/0296120			Khan
		Banavar et al.	2011/0296415 2011/0302154			Khan et al. Snyder
		Fok et al. Holloway et al.	2012/0005276			_
2009/0307133 711 2009/0318171 A1		Backholm et al.	2012/0008536			Tervahauta et al.
	12/2009	•	2012/0022980			Angelone Packbolm et al
2009/0325565 A1 2009/0327390 A1		Backholm Trop et el	2012/0023190 2012/0023226			Backholm et al. Petersen et al.
2009/032/390 A1 2010/0042691 A1		Tran et al. Magnire	2012/0023236			Backholm et al.
2010/0049872 A1		Roskind	2012/0030280			Wang et al.
2010/0057924 A1		Rauber et al.	2012/0054386 2012/0072910			Hanes Martin et al.
2010/0069127 A1 2010/0077035 A1		Fiennes Li et al.	2012/0072910			Backholm
2010/0077033 A1 2010/0077083 A1		Tran et al.	2012/0078996			Shah
2010/0083255 A1		Bane et al.	2012/0096092			Davidge et al.
2010/0087167 A1		Tsurutome et al.	2012/0108225 2012/0110109			Luna et al. Luna et al.
2010/0088722 A1 2010/0093273 A1	4/2010 4/2010	, Q	2012/0110109			Luna et al.
2010/0093273 A1 2010/0115050 A1		Sultenfuss et al.	2012/0110111			Luna et al.
2010/0118190 A1	5/2010	Salfati et al.	2012/0110112			Luna et al.
2010/0131593 A1		Kihara et al.	2012/0110118 2012/0110171			Luna et al. Luna et al.
2010/0131617 A1 2010/0146107 A1	6/2010	Osborne et al. Fiatal	2012/0110171			Luna et al.
2010/0149975 A1		Tripathi et al.	2012/0110174			Wootton et al.
2010/0174735 A1	7/2010		2012/0110275 2012/0130973			Ganti et al. Tamm et al.
2010/0174939 A1 2010/0186011 A1	7/2010		2012/0130973			Luna et al.
2010/0180011 A1 2010/0207870 A1	8/2010	Magenheimer Cho	2012/0131184			Luna et al.
2010/0211651 A1		Guedalia et al.	2012/0135726			Luna et al.
2010/0214984 A1		Cho et al.	2012/0140750 2012/0149352			Yan et al. Backholm et al.
2010/0227594 A1 2010/0228863 A1		DeVries Kawauchi	2012/0145332			Luna et al.
2010/0229095 A1		Maiocco et al.	2012/0157170			Backholm et al.
2010/0238915 A1		Cayla et al.	2012/0158837			Kaul
2010/0250706 A1			2012/0158908 2012/0170496			Luna et al. Yang et al.
2010/0250986 A1 2010/0268757 A1	$\frac{9/2010}{10/2010}$		2012/0173616			Luna et al.
2010/0274983 A1		Murphy et al.	2012/0174220			Rodriguez
		Kuusinen et al.	2012/0176968 2012/0178414			Luna Fiatal
2010/0293335 A1 2010/0299223 A1	11/2010	Muthiah et al.	2012/0170414			Luna et al.
		Jorgensen	2012/0185597	A1 7/	2012	Luna
2010/0319054 A1	12/2010	Mehta et al.	2012/0185918			Backholm et al.
2010/0322124 A1		Luoma et al.	2012/0210121 2012/0226767			Boynton et al. Luna et al.
2010/0325306 A1 2011/0028129 A1		Vimpari et al. Hutchison et al.	2012/0220707			Fleming
2011/0020125 711 2011/0040718 A1		Tendjoukian et al.	2012,022,039	711	2012	1 101111119
2011/0065424 A1	3/2011	Estevez et al.	FC	REIGN E	A TE	NT DOCUMENTS
2011/0066646 A1		Danado et al.				
2011/0099363 A1 2011/0113109 A1		Boynton et al. LeVasseur et al.	EP	1422899		5/2004
2011/0119134 A1		Zivkovic et al.	EP EP	1462975 1466261		9/2004 10/2004
2011/0126060 A1		Grube et al.	EP	1466435		10/2004
2011/0138102 A1 2011/0138402 A1		Glikson et al. Fleming	EP	1482702		12/2004
2011/0153402 A1 2011/0153937 A1		Annamalaisami et al.	EP EP	1815634 1815652		8/2007 8/2007
2011/0158239 A1		Mohaban	EP EP	1817883		8/2007 8/2007
2011/0165889 A1		Fiatal et al.	FI	117152		6/2006
2011/0179138 A1		Van Geest et al.	FI	118288		9/2007
2011/0179377 A1 2011/0182220 A1		Fleming Black et al.	FI JP	119581 4-154233		12/2008 5/1992
ZUII/UIOZZZZU AI	1/ ZUII	DIACK Ct al.	JI	T-134233	,	J/ 1772

(56)	Referen	ces Cited	B'Far, R
	EOREIGN PATE	NT DOCUMENTS	Devices
	TOREIGNIAIL	NI DOCOMENIS	23, 2006 Blaney,
JP	4154233 A	5/1992	Comput
JP	10-336372 A	12/1998	JanFeb
JP	2001-218185 A	8/2001	Braden,
JP	2001-218185	10/2001	port," R
JP JP	2001-350718 A 2001-356973 A	12/2001 12/2001	Brown,
JP	2001-330973 A 2005-515664 T	5/2005	pages, 1
JP	2009-207177 A	9/2009	"Chapte
JP	4386732 B2	10/2009	Publishe
KR	2001-0018568 A	3/2001	"Chapte
KR	2006-0068186 A	6/2006	pages, P
KR KR	2007-0071858 A1 10-0765238 B1	7/2007 10/2007	Cole, Ba
KR	2007-0102091 A1	10/2007	Network "CR 348
KR	2007-0117874 A	12/2007	ing #64,
KR	2009-0077515 A	7/2009	"CR 410
KR	2010-0064605 A	6/2010	Meeting
WO WO	WO 97/41661 WO 97/41661 A2	11/1997 11/1997	Dahl, A
WO	9824257	6/1998	Sams Pu
WO	WO 98/24257 A1	6/1998	Decker,
WO	WO 98/58322	12/1998	prise Re
WO	WO 98/58322 A2	12/1998	pages, N
WO	WO 01/30130 A2	5/2001	Elz, R. e
WO WO	WO 03/007570 A1 WO 03/058483 A1	1/2003 7/2003	pages, J
WO	WO 03/058465 A1	7/2003	Europea
WO	WO 03/065701 A1	8/2003	Europea
WO	03098890	11/2003	Europea Europea
WO	WO 03/098890 A1	11/2003	Europea
WO WO	WO 2004/017591 A2 2004045171	2/2004 5/2004	Europea
WO	WO 2004/045171 A1	5/2004	Falkner,
WO	WO 2005/015925 A2	2/2005	in Your
WO	WO 2005/020108 A1	3/2005	Freeland
WO	WO 2006/045005 A2	4/2006	Worldw
WO WO	WO 2006/045102 A2 WO 2006/053952 A1	4/2006 5/2006	Frenkel,
WO	WO 2006/053954 A1	5/2006	Network Gamelir
WO	WO 2006/058967 A1	6/2006	Gamen Gewirtz
WO	WO 2007/015725 A2	2/2007	pages, 1
WO	WO 2007/015726 A1	2/2007	Grous,
WO WO	WO 2007/149526 A2 WO 2007/149540 A2	12/2007 12/2007	Internot
WO	WO 2008/061042 A2	5/2008	Oct. 199
WO	WO 2011/126889 A2	10/2011	GSM A
WO	WO 2012/018430 A1	2/2012	Best Pra
WO	WO 2012/018431 A1	2/2012	Haas, Z
WO WO	WO 2012/018477 A2 WO 2012/018479 A2	2/2012 2/2012	Protocol
WO	WO 2012/018175 A2	2/2012	Haas, Z TCP for
WO	WO 2012/024030 A2	2/2012	10, pp. 1
WO	WO 2012/060995 A2	5/2012	Hajdu, l
WO	WO 2012/060996 A2	5/2012	Environ
WO WO	WO 2012/060997 A2 WO 2012/061430 A2	5/2012 5/2012	Hardy, E
WO	WO 2012/001430 A2 WO 2012/061433 A2	5/2012	faces," I
WO	WO 2012/061437 A1	5/2012	IBM Co
WO	WO 2012/071283 A1	5/2012	No. 114
WO	WO 2012/071384 A2	5/2012	IBM Co.
WO	WO 2012/094675 A2	7/2012	oper Do
	OTHER PUI	BLICATIONS	ImTOO
			IntelliLi

Android Developers, "Date," 10 pages, Oct. 27, 2011.

Augun, Audrey, "Integrating Lotus Notes With Enterprise Data," Lotus Notes Advisory, pp. 22-25, Jul.-Aug. 1996.

Balaban, Bob, "This Is Not Your Father's Basic: LotusScript in Notes Release 4," The View, vol. 1, Issue 5, 32 pages, Nov.-Dec. 1995.

Bedell, Doug, "Meeting Your New Best Friends Six Degrees Widens Your Contacts In Exchange for Sampling Web Sites," The Dallas Morning News, 4 pages, Oct. 27, 1998.

Bergman, Lawrence D. et al., "Programming-By-Demonstration for Behavior-Based User Interface Customization," IBM Research Report, RC23116, 5 pages, Feb. 20, 2004.

Reza et al., "Designing Effective User Interfaces for Wireless" es," Publication Unknown, 14 pages, Published prior to Feb.

Jeff, "You Can Take It With You—An Introduction to Mobile iting With Notes R4," The View, vol. 2, Issue 1, 14 pages, eb. 1996.

R., "Requirements for Internet Hosts—Application and Sup-RFC 1123, 80 pages, Oct. 1989.

Kevin et al., "Mastering Lotus Notes®," Sybex Inc., 996 1995.

ter: About NotesPump," Publication Unknown, 480 pages, ned prior to Jan. 8, 2003.

ter 13-1—Anatomy of a Note ID," Publication Unknown, 8 Published prior to Jan. 8, 2003.

Barb et al., "Lotus Airs Notes-To-Database Integration Tool," rk World, 2 pages, Oct. 2, 1995.

183 to Release 8 TS 25.331, Rev. 2," 3GPP TSG-RAN2 Meet-I, Prague, Czech Republic, 11 pages, Nov. 10-14, 2008.

100 to Release 8 TS 25.331, Rev. 1," 3GPP TSG-RAN WG2 g #69, San Francisco, U.S., 6 pages, Feb. 22-26, 2010.

Andrew, "Lotus Notes® 4 Administrator's Survival Guide," Publishing, 64 pages, 1996.

, Stefan et al., "The Social Semantic Desktop," Digital Enter-Research Institute, DERI Technical Report 2004-05-02, 7 May 2004.

et al., "Clarifications to the DNS Specification," RFC 2181, 12 Jul. 1997.

ean Patent Application No. EP 03705704.9, Supplementary ean Search Report, 4 pages, Jun. 9, 2010.

ean Patent Application No. EP 03707338.4, Supplementary ean Search Report, 2 pages, Apr. 18, 2011.

ean Patent Application No. EP 05815115.0, Supplementary

ean Search Report, 7 pages, Nov. 17, 2011. r, Mike, "How to Plan, Develop, and Implement Lotus Notes®

Organization," John Wiley & Sons, Inc., 539 pages, 1996. id, Pat et al., "Lotus Notes 3-3.1 for Dummies™," IDG Books wide, 389 pages, 1994.

l, Garry, "Pumping for Info: Notes and Database Integration," rk Computing, 10 pages, May 1, 1996.

ine, Advertisement, 1 page, 1982.

z, David, "Lotus Notes 3 Revealed!," Prima Publishing, 261 1994.

Paul J., "Creating and Managing a Web Site With Lotus otes Web Publisher," The View, vol. 1, Issue 4, 20 pages, Sep.-95.

Association, "Network Efficiency Task Force Fast Dormancy ractices," V1.0, 21 pages, May 26, 2010.

Zygmunt J. et al., "Mobile-TCP: An Asymmetric Transport ol Design for Mobile Systems," IEEE, pp. 1054-1058, 1997.

Zygmunt J. et al., "The Design and Performance of Mobile" r Wireless Networks," Journal of High Speed Networks, vol. 187-207, 2001.

Kalman et al., "Lotus Notes Release 4 in A Multiplatform nment," IBM Corporation, 173 pages, Feb. 1996.

Ed, "Microsoft Proposes Two New Thumb-Driven User Inter-Brighthand Consulting, Inc., 2 pages, 2003.

Corporation, "The Architecture of Lotus Notes," White Paper

4654, 26 pages, May 31, 1995. forporation, "The History of Notes and Domino," Lotus Devel-

omain, 11 pages, Sep. 29, 2003. O, "ImTOO iPod Movie Converter," 3 pages, Nov. 9, 2005. IntelliLink Corporation, "IntelliLink® for Windows User's Guide,"

Version 3.0, 167 pages, 1994. International Application No. PCT/US2003/000618, International Search Report, 1 page, Apr. 4, 2003.

International Application No. PCT/US2003/000624, International Search Report, 2 pages, May 13, 2003.

International Application No. PCT/US2005/037702, International

Preliminary Examination Report, 6 pages, Nov. 20, 2007. International Application No. PCT/US2005/037702, International

Search Report, 1 page, Nov. 5, 2007. International Application No. PCT/US2005/037702, Written Opin-

ion, 6 pages, Nov. 5, 2007.

OTHER PUBLICATIONS

International Application No. PCT/US2005/038135, International Search Report, 2 pages, Aug. 8, 2008.

International Application No. PCT/US2005/038135, Written Opinion, 8 pages, Aug. 8, 2008.

International Application No. PCT/US2005/038135, International Preliminary Report on Patentability, 9 pages, Oct. 31, 2011.

International Application No. PCT/FI2005/050424, International Search Report, 4 pages, Mar. 2, 2006.

International Application No. PCT/FI2005/050426, International Search Report, 3 pages, Mar. 1, 2006.

International Application No. PCT/FI2005/050441, International Search Report, 3 pages, Mar. 1, 2006.

International Application No. PCT/US2006/023426, International Search Report, 1 page, Feb. 21, 2007.

International Application No. PCT/US2006/023427, International Search Report, 1 page, Oct. 12, 2006.

International Application No. PCT/US2007/014462, International Search Report, 1 page, Jul. 2, 2008.

International Application No. PCT/US2007/014497, International Search Report, 1 page, Aug. 25, 2008.

International Application No. PCT/US2011/030534, International Search Report, 10 pages, Dec. 29, 2011.

International Application No. PCT/US2011/037932, International Search Report, 9 pages, Jan. 2, 2012.

International Application No. PCT/US2011/037943, International Search Report, 11 pages, Jan. 2, 2012.

International Application No. PCT/US2011/043322, International Search Report, 9 pages, Feb. 9, 2012.

International Application No. PCT/US2011/043328, International Search Report, 12 pages, Feb. 27, 2012.

International Application No. PCT/US2011/043409, International

Search Report, 11 pages, Feb. 9, 2012. International Application No. PCT/US2011/058840, International Search Report, 10 pages, Apr. 26, 2012.

International Application No. PCT/US2011/058843, International Search Report, 11 pages, May 16, 2012

Search Report, 11 pages, May 16, 2012. International Application No. PCT/US2011/058848, International

Search Report, 10 pages, Apr. 10, 2012. International Application No. PCT/US2011/061512, International

Search Report, 10 pages, May 10, 2012. International Application No. PCT/US2012/022121, International

Search Report, 11 pages, May 14, 2012. Japanese Patent Application No. 2003-558726, Office Action, 2

pages, Jun. 10, 2008. Karlson, Amy K. et al., "AppLens and LaunchTile: Two Designs for One-Handed Thumb Use on Small Devices," Proceedings of CHI

2005, 10 pages, Apr. 2-7, 2005. Kent, S. et al., "Security Architecture for the Internet Protocol," RFC

2401, The Internet Society, 62 pages, Nov. 1998.

Kleinberg, Jon, "The Small-World Phenomenon: An Algorithmic Perspective," Cornell Computer Science Technical Report 99/1776, 14 pages, Oct. 1999.

Koeppel, Dan, "GUIs Just Want To Have Fun," Wired Magazine, Issue 8.10, 12 pages, Oct. 2000.

Kornblith, Polly Russell, "Lotus Notes Answers: Certified Tech Support," Covers Release 3, McGraw-Hill, Inc., 326 pages, 1994.

Kreisle, Bill, "Teach Yourself . . . Lotus Notes 4," MIS Press, 464 pages, 1996.

Lamb, John P. et al., "Lotus Notes Network Design," McGraw-Hill, 278 pages, 1996.

Londergan, Stephen et al., "Lotus Notes® Release 4 For Dummies®," IDG Books Worldwide, 229 pages, 1996.

Lotus Development Corporation, "Firewall Security Overview and How Firewalls Relate to Lotus Notes," Lotus Notes Knowledge Base, 9 pages, May 22, 1996.

Lotus Development Corporation, "How to Set Up 'Firewall' Protection for a Notes Domain," Lotus Notes Knowledge Base, 2 pages, Nov. 6, 1995.

Lotus Development Corporation, "Lotus Announces Lotus NotesPump 1.0," Lotus Notes Knowledge Base, 6 pages, Oct. 31, 1995.

Lotus Development Corporation, "Lotus Inside Notes—The Architecture of Notes and the Domino Server," 207 pages, 2000.

Lotus Development Corporation, "Lotus NotesPump 1.0 Q & A," Lotus Notes Knowledge Base, 3 pages, Oct. 31, 1995.

Lotus Development Corporation, "Lotus NotesPump: Database Integration for Lotus Notes," Lotus Notes Knowledge Base, 5 pages, Oct. 31, 1995.

Lotus Development Corporation, "Lotus Notes Administration," Release 3.3, 20 pages, 1995.

Lotus Development Corporation, "Lotus Notes Administrator's Guide," Release 4, 499 pages, 1995.

Lotus Development Corporation, "Lotus Notes Administrators Guide—Server for NetWare, OS-2, and Unix," Release 3.1, 509 pages, 1994.

Lotus Development Corporation, "Lotus Notes Administrators Guide—Server for Windows," Release 3.1, 345 pages, 1994.

Lotus Development Corporation, "Lotus Notes Application Developer's Guide," Release 4, 475 pages, 1995.

Lotus Development Corporation, "Lotus Notes Customer Service Application Guide," Release 3.1, 46 pages, 1994.

Lotus Development Corporation, "Lotus Notes Customer Support Guide," 33 pages, Published prior to Jan. 8, 2003.

Lotus Development Corporation, "Lotus Notes Customer Support Guide—North American Guide," Release 4.1, 51 pages, Published prior to Jan. 8, 2003.

Lotus Development Corporation, "Lotus Notes Database Manager's Guide," Release 4, 115 pages, 1995.

Lotus Development Corporation, "Lotus Notes Deployment Guide," Release 4, 104 pages, 1995.

Lotus Development Corporation, "Lotus Notes for Windows, OS-2, and Macintosh," Release 3.3, 89 pages, 1995.

Lotus Development Corporation, "Lotus Notes Getting Started With Application Development," Release 3.1, 151 pages, 1994.

Lotus Development Corporation, "Lotus Notes Install Guide for Servers," Release 4, 68 pages, 1996.

Lotus Development Corporation, "Lotus Notes Install Guide for Workstations," Release 4, 28 pages, 1995.

Lotus Development Corporation, "Lotus Notes Install Guide for Workstations," Release 4.1, 67 pages, 1996.

Lotus Development Corporation, "Lotus Notes Install Guide for

Workstations," Release 4.5, 81 pages, 1996. Lotus Development Corporation, "Lotus Notes Internet Cookbook for Notes Release 3," 21 pages, Jan. 16, 1996.

Lotus Development Corporation, "Lotus Notes Internet Cookbook for Notes Release 4," 35 pages, Feb. 14, 1996.

Lotus Development Corporation, "Lotus Notes Internotes Web Navigator Administrator's Guide," Release 4, 60 pages, 1995.

Lotus Development Corporation, "Lotus Notes Internotes Web Navigator User's Guide," Release 4, 56 pages, 1995.

Lotus Development Corporation, "Lotus Notes Internotes Web Publisher Guide," Release 4, 122 pages, 1996.

Lotus Development Corporation, "Lotus Notes LotusScript Classes for Notes," Release 4, 6 pages, Published prior to Jan. 8, 2003.

Lotus Development Corporation, "Lotus Notes Migration Guide," Release 4, 110 pages, 1996.

Lotus Development Corporation, "Lotus Notes Network Configuration Guide," Release 4.5, 121 pages, 1996.

Lotus Development Corporation, "Lotus Notes Network Driver Documentation," Release 3.1, 100 pages, 1994.

Lotus Development Corporation, "Lotus Notes Programmers Guide—Part 1," Release 4, 614 pages, 1995.

Lotus Development Corporation, "Lotus Notes Programmers Guide—Part 2," Release 4, 462 pages, 1995.

Lotus Development Corporation, "Lotus Notes Quick Reference for Application Developers," Release 3, 6 pages, Published prior to Jan. 8, 2003.

Lotus Development Corporation, "Lotus Notes Quick Reference for Macintosh," Release 3, 6 pages, Published prior to Jan. 8, 2003. Lotus Development Corporation, "Lotus Notes Quick Reference for

SmartIcons," Release 3.1, 4 pages, Published prior to Jan. 8, 2003.

OTHER PUBLICATIONS

Lotus Development Corporation, "Lotus Notes Quick Reference for Windows and Presentation Manager," Release 3, 6 pages, Published prior to Jan. 8, 2003.

Lotus Development Corporation, "Lotus Notes Release Notes," Release 4, 139 pages, 1995.

Lotus Development Corporation, "Lotus Notes Release Notes," Release 4.1, 197 pages, 1996.

Lotus Development Corporation, "Lotus Notes Server for Windows," Release 3.3, 7 pages, 1994.

Lotus Development Corporation, "Lotus Notes Server Up and Running!," Release 4, 13 pages, 1996.

Lotus Development Corporation, "Lotus Notes Site and Systems Planning Guide," Release 3.1, 169 pages, 1994.

Lotus Development Corporation, "Lotus Notes Start Here—Workstation Install for Windows, OS-2 and Macintosh," Release 3.3, 47 pages, 1995.

Lotus Development Corporation, "Lotus Notes Step by Step—A Beginner's Guide to Lotus Notes," Release 4, 179 pages, 1995.

Lotus Development Corporation, "Lotus Notes Step by Step—A Beginner's Guide to Lotus Notes," Release 4.1, 167 pages, 1996.

Lotus Development Corporation, "Lotus Software Agreement," 8 pages, Published prior to Jan. 8, 2003.

Lotus Development Corporation, "What Is the Notes Replicator?," Lotus Notes Knowledge Base, 8 pages, Jul. 5, 1995.

"Lotus Notes Advisor," Advisor Publications Inc., 55 pages, Jun. 1995.

"Lotus Notes Advisor," Advisor Publications Inc., 55 pages, Aug. 1995.

"Lotus Notes Advisor," Advisor Publications Inc., 55 pages, Oct. 1995.

"Lotus Notes Advisor," Advisor Publications Inc., 55 pages, Dec. 1995.

"Lotus Notes Advisor," Advisor Publications Inc., 63 pages, Jan.-Feb. 1996.

"Lotus Notes Advisor," Advisor Publications Inc., 55 pages, Apr. 1996.

"Lotus Notes Advisor," Advisor Publications Inc., 55 pages, Jun. 1996.

"Lotus Notes Advisor," Advisor Publications Inc., 55 pages, Aug. 1996.

"Lotus Notes Advisor," Advisor Publications Inc., 55 pages, Oct. 1996.

"Lotus Notes Advisor," Advisor Publications Inc., 63 pages, Dec. 1996.

"Lotus Notes—Notes Administration Help," Screen Shots, 17 pages, Published prior to Jan. 8, 2003.

MacGregor, Rob et al., "The Domino Defense: Security in Lotus Notes and the Internet," IBM Corporation, 183 pages, Dec. 1997.

Maltz, David A. et al., "MSOCKS: An Architecture for Transport Layer Mobility," IEEE, pp. 1037-1045, 1998.

Marmel, Elaine, "Easy Lotus® Notes Release 4.0," Que Corporation, 237 pages, 1996.

Mason, Luke, "Windows XP: New GUI Design Shows Skin Is In," TechRepublic, 4 pages, Apr. 4, 2001.

Microsoft, Definition of "Access," Microsoft Computer Dictionary, Fifth Edition, 2 pages, May 1, 2002.

Microsoft, Definition of "Synchronization," Microsoft Computer Dictionary, Fifth Edition, 2 pages, May 1, 2002.

Milgram, Stanley, "The Small-World Problem," Psychology Today, vol. 2, pp. 60-67, 1967.

Miller, Victor S., "Use of Elliptic Curves in Cryptography," Advances in Cryptology—CRYPTO '85 Proceedings, vol. 218, pp. 417-426, 1985.

Mockapetris, P., "Domain Names—Concepts and Facilities," RFC 1034, 43 pages, Nov. 1987.

Mockapetris, P., "Domain Names—Implementation and Specification," RFC 1035, 43 pages, Nov. 1987.

Myers, Brad A. et al., "Extending The Windows Desktop Interface With Connected Handheld Computers," WSS'00 Proceedings of the 4th Conference on USENIX Windows Systems Symposium, vol. 4, 10 pages, 2000.

Myers, Brad A. et al., "User Interfaces That Span Hand-Held and Fixed Devices," CHI'2001 Workshop on Distributed and Disappearing User Interfaces in Ubiquitous Computer, 4 pages, 2001.

National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," Federal Information Processing Standards Publication 197, 52 pages, Nov. 26, 2001.

National Institute of Standards and Technology, "Secure Hash Standard," Federal Information Processing Standards Publication 180-2, 83 pages, Aug. 1, 2002.

Netscape Communications Corporation, "Netscape Mail Server Administrator's Guide," Version 2.0, 172 pages, 1996.

Netscape Communications Corporation, "Netscape Mail Server Installation Guide," Version 2.0 for Unix, 62 pages, 1996.

Netscape Communications Corporation, "Netscape Mail Server User's Guide," Version 2.0, 35 pages, 1996.

Netscape Communications Corporation, "Netscape News Server Administrator's Guide for Windows NT," Version 2.0, 119 pages, 1996.

Niederée, Claudia et al., "A Multi-Dimensional, Unified User Model for Cross-System Personalization," Proceedings of the AVI 2004 Workshop on Environments for Personalized Information Access, 11 pages, 2004.

Nokia, "Developer Platforms," 3 pages, 2005.

"NotesPump 1.0 Release Notes," Publication Unknown, 8 pages, Published prior to Jan. 8, 2003.

Opyt, Barbara et al., "Use the Internet As Your Lotus Notes WAN," Lotus Notes Advisor, pp. 17-20, Nov.-Dec. 1996.

Ortiz, C. Enrique, "An Introduction to the Symbian OS™ Platform for Palm OS® Developers," Metrowerks Corp., 21 pages, 2002.

"Overview—What Is Lotus NotesPump?," Publication Unknown, 88 pages, Published prior to Jan. 8, 2003.

Perez, Sarah, "Onavo's Data-Compressing Mobile App Raises \$10 Million Series B From Horizons, Motorola Ventures," 2 pages, Jan. 24, 2012.

Pyle, Hugh, "The Architecture of Lotus Notes," Lotus Notes Advisor, Premiere Issue, pp. 18-27, 1995.

Pyle, Lisa, "A Jump Start to the Top Ten R3-To-R4 Migration Considerations," The View, vol. 1, Issue 5, 22 pages, Nov.-Dec. 1995.

Qualcomm Incorporated, "Managing Background Data Traffic in Mobile Devices," 16 pages, Jan. 2012.

Qualcomm, "System Parameter Recommendations to Optimize PS Data User Experience and UE Battery Life," 80-W1112-1, Revision B, 9 pages, Mar. 2007.

Ringel, Meredith et al., "iStuff: A Scalable Architecture for Light-weight, Wireless Devices for Ubicomp User Interfaces," Proceedings of UbiComp 2002, 2 pages, 2002.

Signorini, Eugene, "Seven's Service-Based Wireless Solutions Enable Enterprises to Untether E-Mail," Wireless/Mobile Enterprise & Commerce, 16 pages, Oct. 2004.

Swedeen, Bret et al., "Under The Microscope—Domino Replication," LDD Today, 8 pages, Oct. 1, 1998.

Tamura, Randall A., "Lotus® Notes™ 4 Unleashed," Sams Publishing, 928 pages, 1996.

U.S. Appl. No. 60/663,463, File History, 113 pages, Mar. 18, 2005. Vivacqua, Adriana et al., "Profiling and Matchmaking Strategies In Support Of Opportunistic Collaboration," CoopIS/DOA/ODBASE 2003, LNCS 2888, pp. 162-177, 2003.

Wainwright, Andrew, "Secrets to Running Lotus Notes: The Decisions No One Tells You How to Make," IBM Corporation, 193 pages, Oct. 1996.

Wilcox, Adam A., "PC Learning Labs Teaches Lotus Notes 3.0," Ziff-Davis Press, 381 pages, 1993.

Wong, Harry, "Casahl's Replic-Action: Delivering True Notes-DBMS Integration," The View, vol. 2, Issue 1, pp. 33-50, Jan.-Feb. 1996.

Eronen, "TCP Wake-Up: Reducing Keep-Alive Traffic in Mobile IPv4 and Ipsec NAT Traversal," NRC-TR-2008-002, Nokia, 10 pages, Jan. 31, 2008.

OTHER PUBLICATIONS

European Patent Application No. EP 03707338.4, Examination Report, 4 pages, Sep. 9, 2011.

European Patent Application No. EP 05813041.0, Supplementary European Search Report & Examination Report, 10 pages, Apr. 25, 2013.

European Patent Application No. EP 05813045.1, Supplementary European Search Report & Examination Report, 6 pages, Apr. 9, 2013.

International Application No. PCT/US2011/044974, International Search Report & Written Opinion, 15 pages, Jun. 1, 2012.

International Application No. PCT/US2011/056474, International Search Report & Written Opinion, 9 pages, May 4, 2012.

International Application No. PCT/US2011/056476, International Search Report & Written Opinion, 12 pages, May 24, 2012.

International Application No. PCT/US2011/056478, International Search Report & Written Opinion, 11 pages, May 31, 2012.

International Application No. PCT/US2011/061795, International Search Report & Written Opinion, 10 pages, Jul. 31, 2012.

International Application No. PCT/US2012/020669, International Search Report & Written Opinion, 10 pages, Sep. 12, 2012.

International Application No. PCT/US2012/021459, International Search Report & Written Opinion, 10 pages, Jun. 1, 2012.

Newton, Harry, "Newton's Telecom Dictionary," 20th Edition, pp. 67, 127, 542, Mar. 2004.

Phillips, Joshua et al., "Modeling the Intelligence Analysis Process for Intelligent User Agent Development," Research and Practice in Human Resource Management, vol. 9, No. 1, pp. 59-73, 2001.

Seven Networks, Inc., "Seven Optimizing the Mobile Ecosystem," www.seven.com/products.traffic_optimization.php, 1 page, May 29, 2012.

Wikipedia, Definition for "General Packet Radio Service," 7 pages, downloaded on May 31, 2012.

Lotus Development Coporation, Lotus Notes Release 3.1: The Groupware Standard, Site and Systems Planning Guide 1991.

Lotus Development Corporation, Lotus Notes: The Groupware Standard—Windows, 1994.

International Search Report for PCT/US03/00618, Date of completion Mar. 19, 2003; Date of Mailing Apr. 4, 2003; ISA/US.

International Search Report for PCT/US03/00624, Date of completion Apr. 8, 2003; Date of Mailing May 13, 2003; ISA/US.

International Search Report for PCT/US05/038135, Date of completion Jan. 30, 2007; Mailing Date Aug. 8, 2008; ISA/US.

International Search Report for PCT/US05/37702, Date of completion Oct. 24, 2007; Date of Mailing Nov. 5, 2007; ISA/US.

International Preliminary Examination Report for PCT/US05/37702, Date of completion Nov. 20, 2007; ISA/US.

Written Opinion of the International Searching Authority for PCT/US05/37702; Date of completion Oct. 24, 2007; Date of mailing Nov. 5, 2007; ISA/US.

Written Opinion of the International Searching Authority for PCT/US05/38135; Date of completion Jul. 14, 2008; Date of mailing Aug. 8, 2008; ISA/US.

Stolowitz Ford Cowger, LLP, Listing of Related Cases, Jul. 13, 2009. Victor S. Miller, "Use of Elliptic Curves in Cryptography", Lecture Notes in Computer Science, May 21, 1986, vol. 218, p. 417-426, Advances in Cryptology-Crypto' 85.

Netscape Communications Corporation, Administrator's Guide, Netscape Mail Server, Version 2.0, 1995.

IBM, "The Architecture of Lotus Notes," White Paper No. 114654, modified date: May 31, 1995.

Lotus Development Corporation, Lotus Notes Knowledge Base, "What is the Notes Replicator", Jul. 5, 1995.

Grous, Paul J., "Creating and Managing a Web Site with Lotus' InterNotes Web Publisher", The View Technical Journal for Lotus Notes® Software, vol. 1 Issue 4, Sep./Oct. 1995, pp. 3-18.

Cole, Barb et al., "Lotus airs Notes-to-database integration tool," www.looksmart.com, Oct. 2, 1995.

Lotus Development Corporation, Lotus Notes Knowledge Base, "Lotus Announces Lotus NotesPump 1.0", Oct. 31, 1995.

Lotus Development Corporation, Lotus Notes Knowledge Base, "Lotus NotesPump 1.0 Q & A", Oct. 31, 1995.

Lotus Development Corporation, Lotus Notes Knowledge Base, "Lotus NotesPump: Database Integration for Lotus Notes", Oct. 31, 1995.

Lotus Development Corporation, Lotus Notes Knowledge Base, "How to Set Up "Firewall" Protection for a Notes Domain", Nov. 6, 1995.

Lotus Development Corporation, Lotus Notes Release 4 Install Guide for Workstations, First Revision, 1996.

Lotus Development Corporation, Lotus Step by Step: A Beginner's Guide to Lotus Notes, First Revision, 1996.

Freeland, Pat and Londergan, Stephen, Lotus Notes Release 4 for DummiesTM, IDG Books Worldwide, 1996.

Kreisle, Bill, Teach Yourself . . . Lotus Notes 4, MIS:Press, 1996.

Marmel, Elain, Easy Lotus® Notes Release 4.0, Que Corporation, 1996.

Lotus Development Corporation, Lotus Notes Server Up and Running!, Release 4, 1996.

Falkner, Mike, "How to Plan, Develop, and Implement Lotus Notes in Your Organization", Wiley Computer Publishing, John Wiley and Sons, Inc., 1996.

Lamp, John P., et al., "Lotus Notes Network Design", McGraw-Hill, 1996.

Tamura, Randall, A., et al., Lotus Notes 4 Unleashed, Sams Publishing, 1996.

Lotus Development Corporation, Lotus Notes Internet Cookbook for Notes Release 3, Jan. 16, 1996.

Wong, Harry, "Casahl's Replic-Action: Delivering True Notes/DBMS Integration", The View Technical Journal for Lotus Notes® Software, vol. 2, Issue 1, Jan./Feb. 1996, pp. 33-50.

IBM International Technical Support Organization, Lutos Notes Release 4 In a Multiplatform Environment, Feb. 1996.

Lotus Development Corporation, Lotus Notes Internet Cookbook for Notes Release 4, Feb. 14, 1996.

Frenkel, Garry, "Pumping for Info: Notes and Database Integration", Network Computing, May 1, 1996, pp. 76-84.

Lotus Development Corporation, Lotus Notes Knowledge Base, "Firewall Security Overview and How Firewalls Relate to Lotus Notes", May 22, 1996.

IBM Corporation, Secrets to Running Lotus Notes: The Decisions No One Tells You How to Make, Oct. 1996.

Swedeen, Bret, et al., "Under the Microscope: Domino Replication", LDD Today, Oct. 1, 1998.

Lotus Development Corporation, Lotus Inside Notes: The Architecture of Notes and the Domino Server, 2000.

Lotus Software Agreement for "Notes 4.0 NA DKTP Client UPG", Part No. 38985, Date unknown.

Lotus Development Corporation, Lotus Notes Release 3.1: Administrator's Guide—Server for Windows, 1993.

Pyle, Hugh, "The Architecture of Lotus Notes", Lotus Notes Advisor, Advisor Publication, Premier Issue 1995, pp. 18-27.

Lotus Notes Advisor, Advisor Publications, Jun. 1995, entire magazine.

Lotus Notes Advisor, Advisor Publications, Aug. 1995, entire magazine.

Lotus Notes Advisor, Advisor Publications, Oct. 1995, entire magazine.

Balaban, Bob, "This Is Not Your Fathers Basic: LotusScript in Notes Release 4", Lotus Notes Advisor, Advisor Publications, vol. 1, No. 5, Nov.-Dec. 1995, pp. 31-58.

Pyle, Lisa, "A Jump Start to the Top Ten R3-to-R4 Migration Considerations", Lotus Notes Advisor, Advisor Publications, vol. 1, No. 5, Nov.-Dec., pp. 3-20.

Lotus Notes Advisor, Advisor Publications, Dec. 1995, entire magazine.

Dahl, Andrew, Lotus Notes 4 Administrator's Survical Guide, Sams Publishing, 1996.

Netscape Communications Corporation, Administrator's Guide, Netscape News Server, Version 2.0, 1996.

Lotus Notes Advisor, Advisor Publications, Jan./Feb. 1996, entire magazine.

OTHER PUBLICATIONS

Blaney, Jeff, "You Can Take it with you: An Introduction to Mobile Computing with Notes R4," The View Technical Journal for Lotus Notes® Software, vol. 2, Issue 1, Jan./Feb. 1996, pp. 22-32.

Lotus Notes Advisor, Advisor Publications, Apr. 1996, entire magazine.

Lotus Notes Advisor, Advisor Publications, Jun. 1996, entire magazine.

Augun, Audry, "Integrating Lotus Notes With Enterprise Data," Lotus Notes Advisor, Advisor Publications, Jul./Aug. 1996, pp. 22-25.

Lotus Notes Advisor, Advisor Publications, Aug. 1996, entire magazine.

Lotus Notes Advisor, Advisor Publications, Oct. 1996, entire magazine.

Opyt, Barbara et al., "Use the Internet as Your Lotus Notes WAN", Lotus Notes Advisor, Advisor Publications, Nov./Dec. 1996, pp. 17-20.

Lotus Notes Advisor, Advisor Publications, Dec. 1996. entire magazine.

"The History of Notes and Domino", Lotus Developer Domain, Lotus, Sep. 29, 2003.

Lotus NotesPump miscellaneous paper, date unkown.

NotesPump 1.0 Release Notes, date unknown.

Lotus Notes-Notes Administration Help screen shot, date unknown. Chapter 13-1, publication unknown, "Anantomy of a Note ID", date unknown.

Chapter: About NotesPump, publication unknown, date unknown. Lotus Development Corporation, Lotus Quick Reference for SmartIcons, Lotus Notes Release 3.1, Date unknown.

Lotus Development Corporation, Lotus Quick Reference for Windows and Presentation Manager, Lotus Notes Release 3, Date unknown.

Lotus Development Corporation, Lotus Quick Reference for Macintosh, Lotus Notes Release 3.0, Date unknown.

Lotus Development Corporation, Lotus Quick Reference for Application Developer's, Lotus Notes Release 3, Date Unknown.

Lotus Development Corporation, Lotus Customer Support Service, Lotus Notes Customer Support Guides, Date Unknown.

Lotus Development Corporation, Lotus Notes 3.3, Lotus Customer Support, North American Guide, 29 pages, Date unknown.

Lotus Development Corporation, Lotus Notes 4.0, Lotus Customer Support, North American Guide, 29 pages, Date unknown.

Lotus Development Corporation, Lotus Notes 4.1 Starter Pack; Lotus Customer Support, North American Guide, 51 pages, Date unknown. Lotus Development Corporation, "Lotus Script Clases for Notes Release 4", 6 pages, date unknown.

Allchin, James E., "An Architecture for Reliable Decentralized Systems", UMI Dissertation Services, Copyright 1983.

Lotus Development Corporation, Lotus Notes Release 3.1: The Groupware Standard, Administrator's Guide—Server for NetWare, OS/2, and UNIX, 1989.

Lotus Development Corporation, Lotus Notes 3.0: The Quick and Easy Way to Learn, Ziff-Davis Press, 1993.

Lotus Development Corporation, Lotus Notes Release 3.3: Start Here, Workstation Install for Windows, OS/2 and Macintosh, 1993. Lotus Development Corporation, Lotus Notes Release 3.1: The Groupware Standard, Customer Services Application Guide, 1994. Lotus Development Corporation, Lotus Notes Release 3.1: The Groupware Standard, Getting Started with Application Development, 1994.

Lotus Development Corporation, Lotus Notes Release 3.1: The Groupware Standard, Network Driver Documentation, 1994.

Kornblith, Polly R., Lotus Notes Answers: Certified Tech Support, Covers Lotus Notes Release 3, Osborne McGraw-Hill, 1994.

Freeland, Pat and Londergan, Stephen, Lotus Notes 3/3.1 for DummiesTM, IDG Books Worldwide, 1994.

Gewirtz, David, Lotus Notes 3 Revealed! Your Guide to Managing Information and Improving Communication Throughhout Your Organization, Prima Publishing, 1994.

Shafran, Andrew B., Easy Lotus notes for WindowsTM, Que® Corporation, 1994.

Lotus Development Corporation, Lotus Notes Release 3.3: The Groupware Standard, Administration, 1994.

McMullen, Melanie, Editor, Network Remote Access and Mobile Computing, Miller Freeman Inc., 1994.

Lotus Development Corporation, Lotus Notes: The Groupware Standard—Windows, Version 3.3, 1994.

IntelliLink Corporation, IntelliLink® For Windows User's Guide, Version 3.0, 1994.

Lotus Development Corporation, Lotus Notes Release 4: InterNotes Web Navigator Administrator's Guide, 1995.

Lotus Development Corporation, Lotus InterNotes Release 4 Web Publisher: InterNotes Web Publisher Guide, 1995.

Lotus Development Corporation, Lotus Notes Release 4 Install Guide for Servers, 1995.

Lotus Development Corporation, Lotus Notes Release 4.1 Release Note, 1995.

Lotus Development Corporation, Lotus Notes Release 4 Migration Guide, 1995.

Lotus Development Corporation, Lotus Notes Release 4 Database

Manager's Guide, 1995. Lotus Development Corporation, Lotus Notes Release 4 Install

Guide for Workstations, 1995. Lotus Development Corporation, Lotus Step by Step: A Beginner's

Guide to Lotus Notes, 1995.

Lotus Development Corporation, Lotus Notes Release 4 Programmer's Guide Part 1, 1995.

Lotus Development Corporation, Lotus Notes Release 4 Programmer's Guide Part 2, 1995.

Lotus Development Corporation, Lotus Notes Release 4 Administrator's guide, 1995.

Guide, 1995.
Lotus Development Corporation, Lotus Notes Release 4 Application

Lotus Development Corporation, Lotus Notes Release 4 Deployment

Lotus Development Corporation, Lotus Notes Release 4 Application Developer's Guide, 1995.

Lotus Development Corporation, Lotus Notes Release 4 InterNotes Web Navigator User's Guide, 1995.

Lotus Development Corporation, Lotus Notes Release 4 Release Notes, 1995.

Lotus Development Corporation, Lotus Notes Release 4.5 Install Guide for Workstaion, 1995.

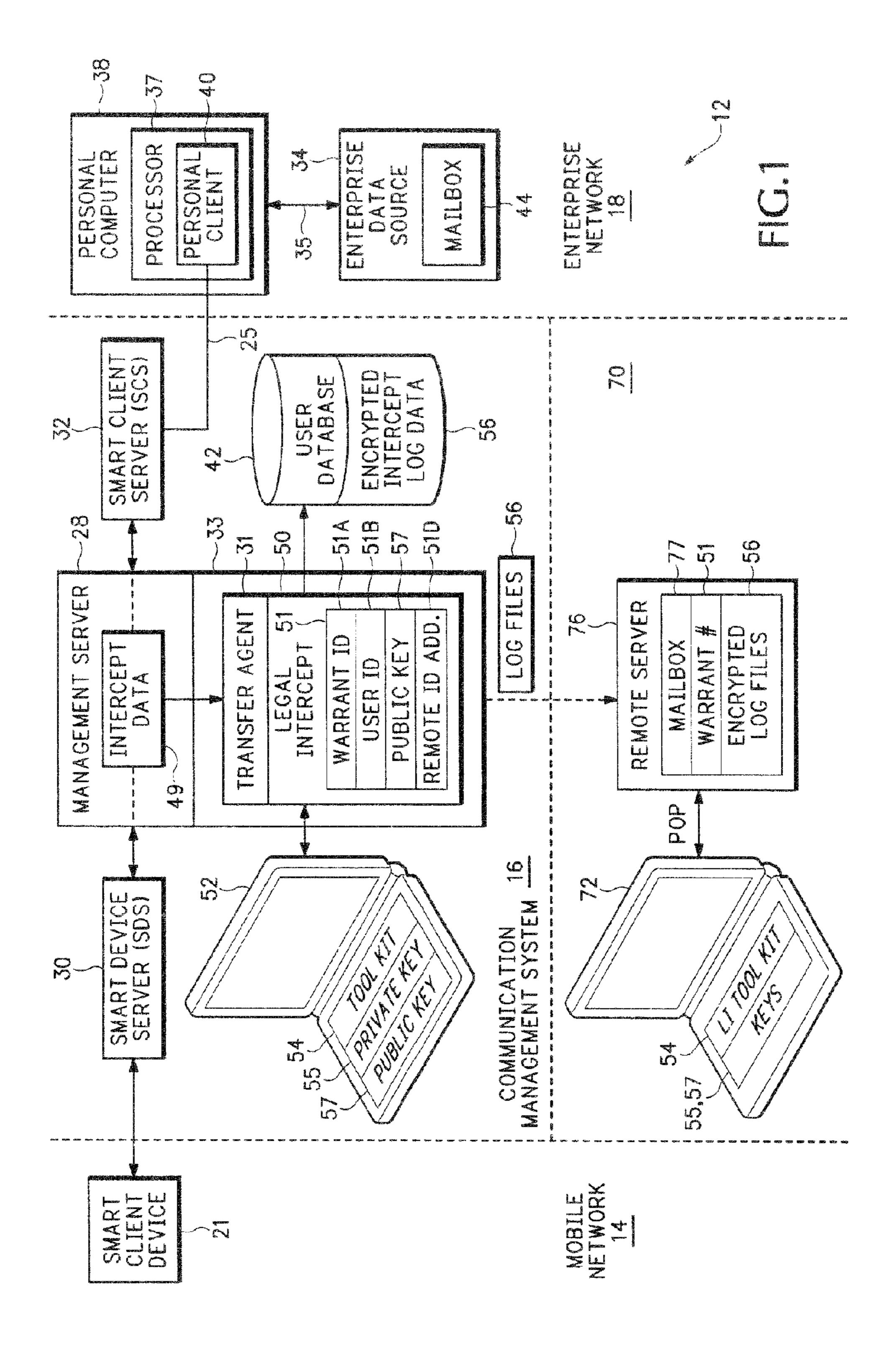
Lotus Development Corporation, Release Notes, Lotus Notes Release 3.30, Windows, OS/2, and Macintosh, 1995.

Brown, Kevin, et al., Mastering Lotus® Notes®, SYBEX Inc., 1995. Lotus Development Corporation, Lotus Notes Release 4.5, Network Configuration Guide, 1995.

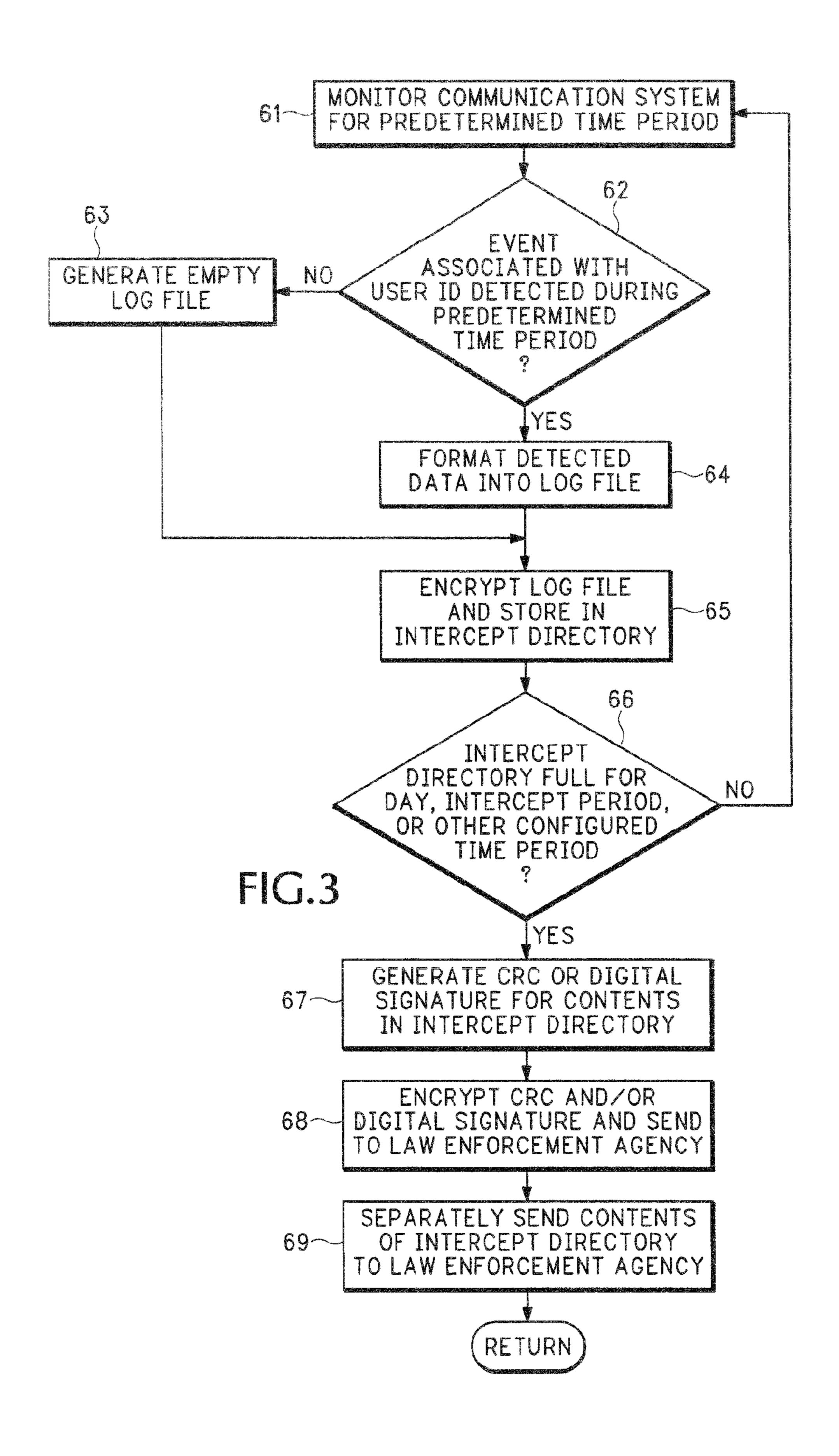
Netscape Communications Corporation, Installation Guide, Netscape Mail Server, Version 2.0 for Unix, 1995.

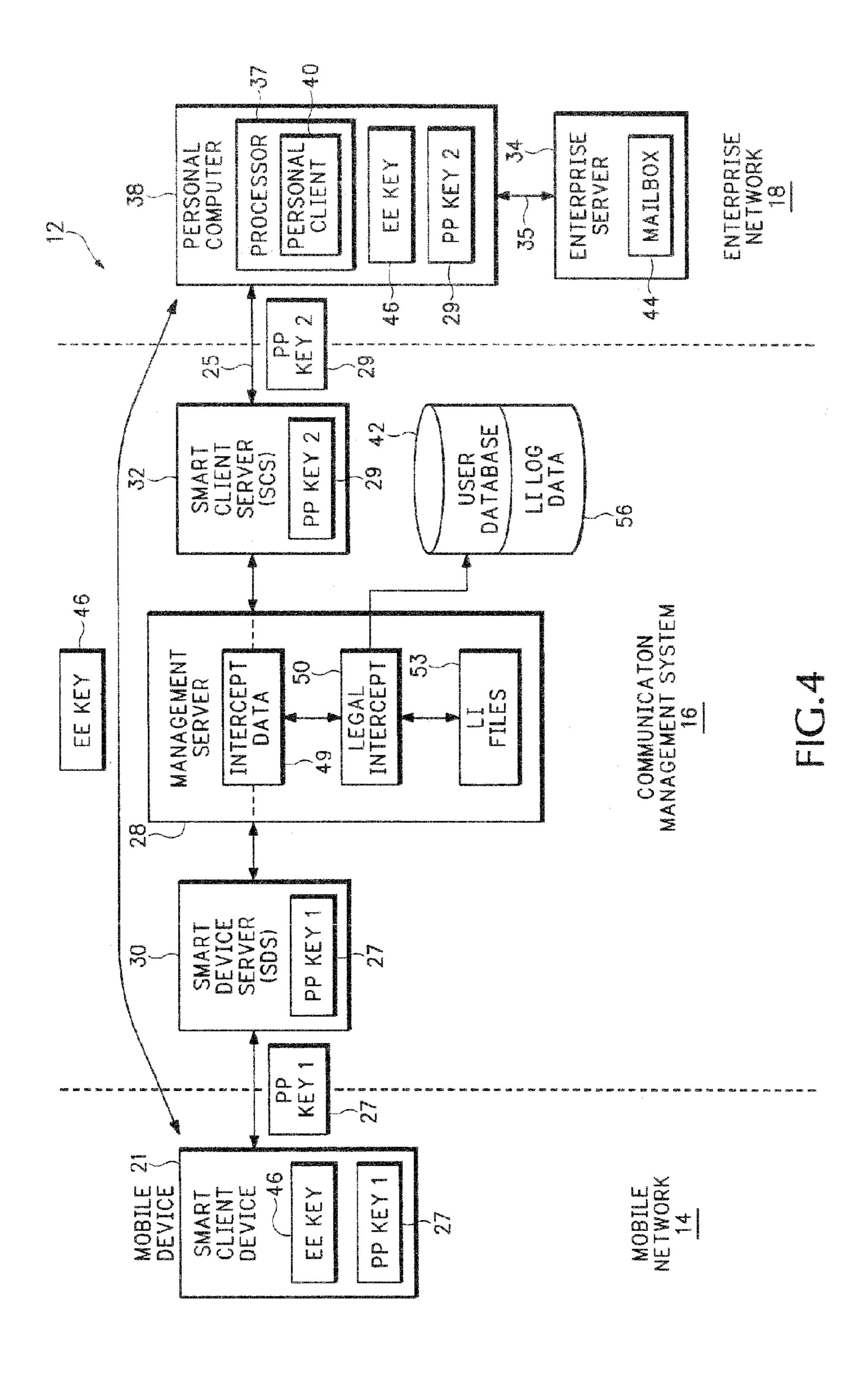
Netscape Communications Corporation, User's Guide, Netscape Mail Server, Version 2.0 for Unix, 1995.

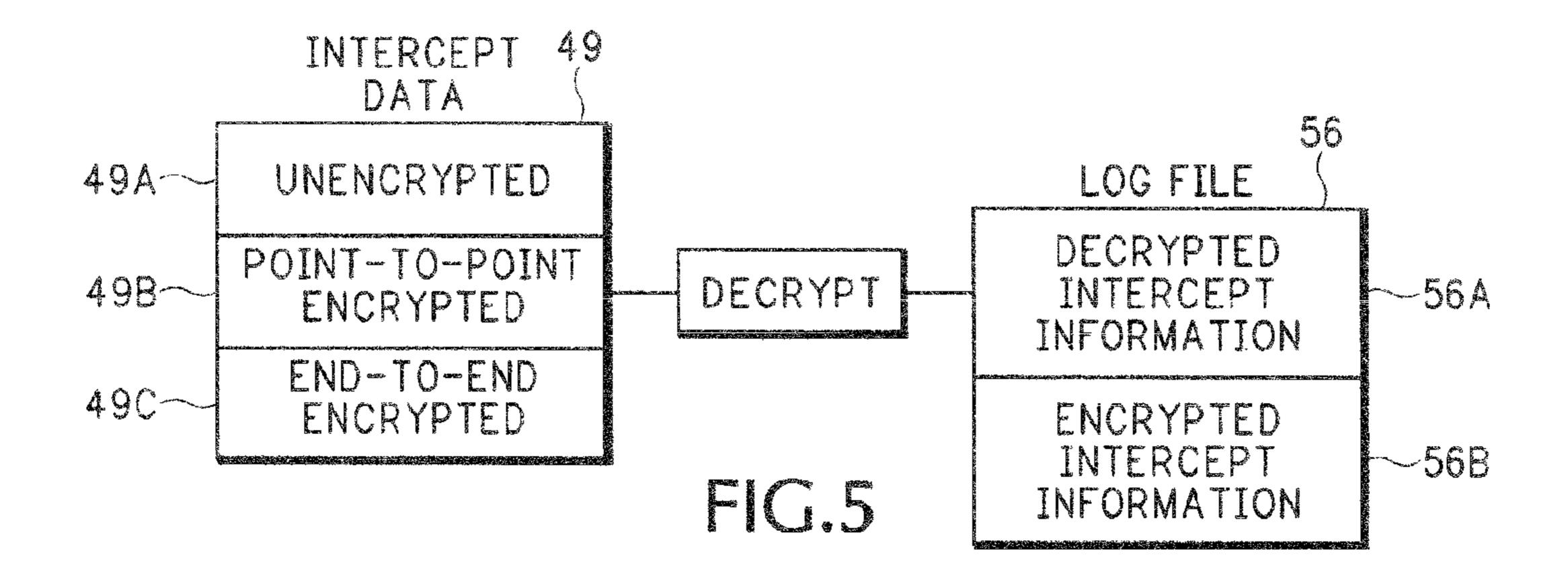
* cited by examiner

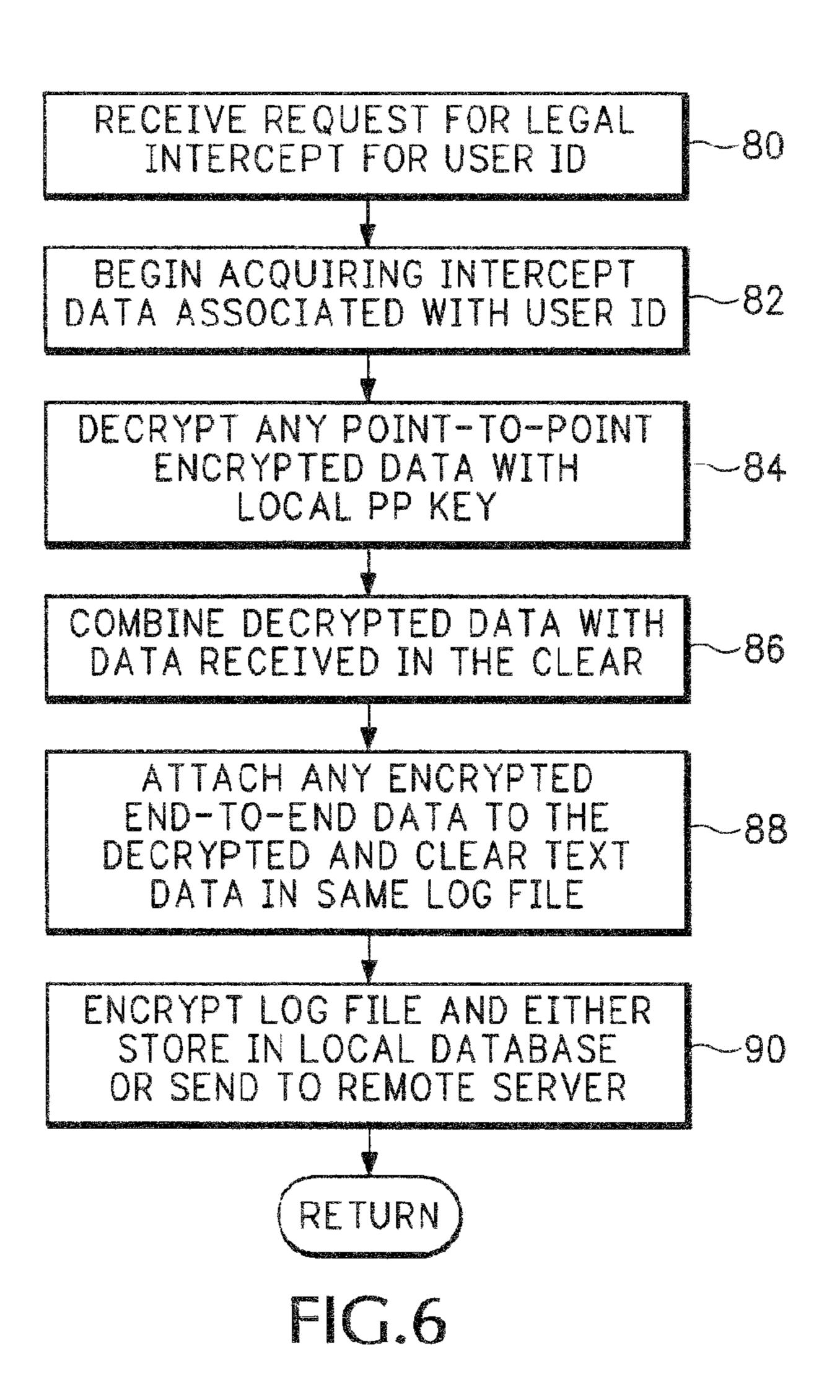


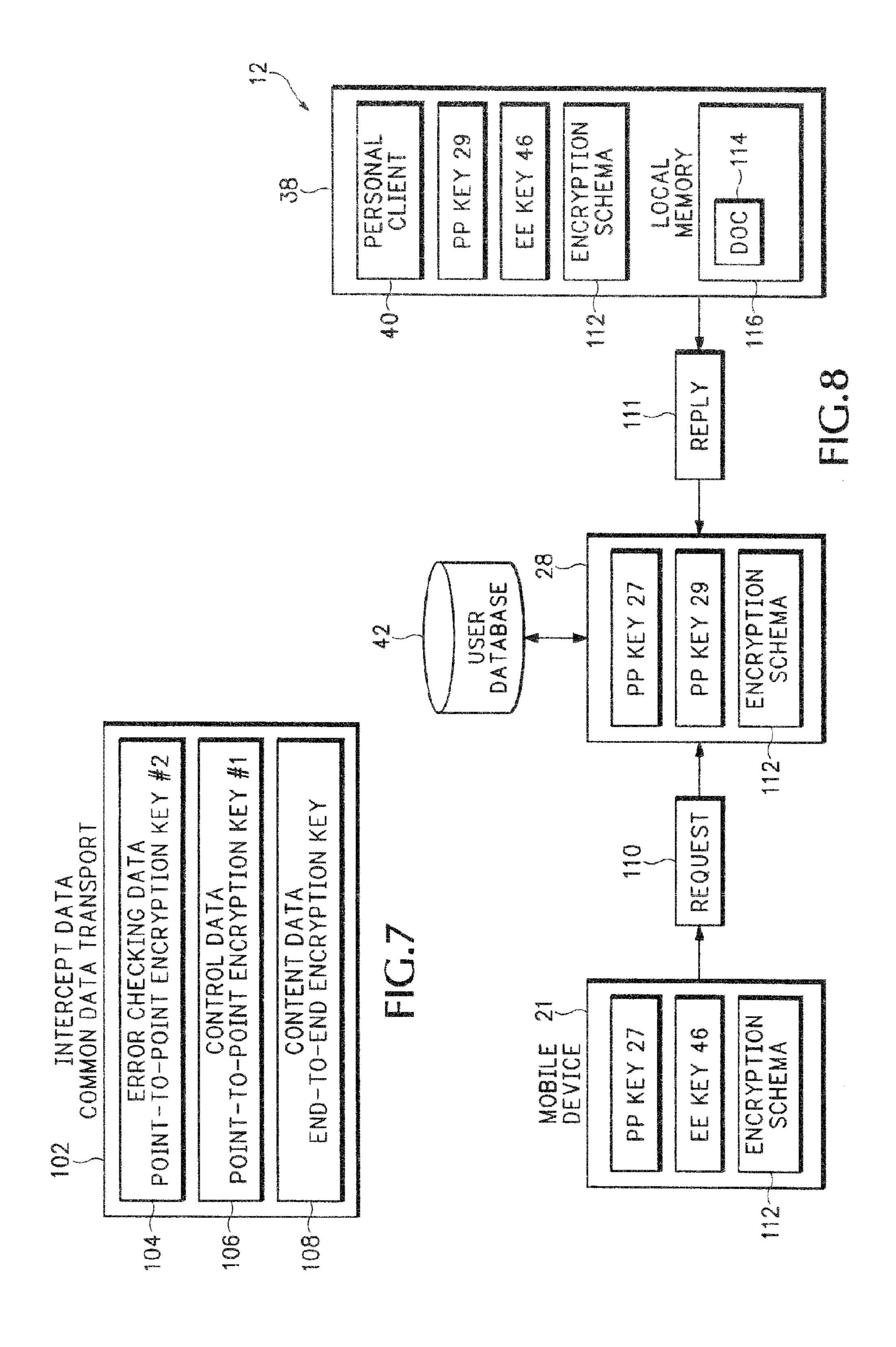
ARANT D-E	FPT/TREVOR SMITH/2005.09.23 NCRYPTION KEY—51C 56A feØ-20050923-00:00.ASC 0 EVENTS LOGGED IN LAST MINUTE 56B
	feØ-20050923-00:01.ASC — 0 EVENTS LOGGED IN LAST MINUTE 56C
	feø-20050923-23:59.ASC











METHOD AND APPARATUS FOR INTERCEPTING EVENTS IN A COMMUNICATION SYSTEM

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; a claim printed with strikethrough indicates that the claim was canceled, disclaimed, or held 10 invalid by a prior post-patent action or proceeding.

CROSS REFERENCE TO RELATED APPLICATIONS

[The present] This patent application is a reissue application for commonly assigned U.S. Pat. No. 7,680,281, issued from U.S. patent application Ser. No. 12/211,790, filed on Sep. 16, 2008, which is a continuation of U.S. patent application Ser. No. 11/255,291, filed on Oct. 20, 2005, now U.S. Pat. No. 7,441,271, which claims priority to U.S. Provisional Patent Application No. 60/620,889, filed on Oct. 20, 2004, each of which are hereby incorporated by reference in their entirety.

BACKGROUND

Wireless digital communication systems wirelessly transport electronic mail (email), text messages, text files, images, Voice Over Internet Protocol (VoIP) data, and any other types of digital data and communications to wireless devices. Wireless communication system providers are facing the prospects of having to comply with a variety of legal-intercept (wiretap) requirements. Authorization for a legal intercept 35 may include warrants for "wiretap/interception", "search and seizure", or both. For example, the requirements outlined in CALEA (US Communications Assistance for Law Enforcement Act of 1994, http://www.askcalea.net/) may have to be met by any proposed solution. In another example, the requirements outlined by the Australian Communications Authority (http://www.aca.gov.au) in the Australia Telecommunications Act of 1997 may have to be met by any proposed solution.

There are several technical challenges complying with these legal intercept requirements that may not exist in conventional telephone systems. For example, the intercepted data may be encrypted. The wireless network provider must be able to intercept the encrypted data, and any other nonencrypted information, without tipping off the intercept target that the wiretap is taking place.

The wiretap warrant may require the communication system provider to provide any intercepted information in substantially real-time or may require the communication system provider to intercept and store communications in an automated manner for later retrieval and analysis by the law enforcement agency. Evidentiary problems exist with information intercepted outside the presence and control of the enforcement agency. For example, the intercepted communications could be either intentionally or inadvertently deleted. A system malfunction could also prevent some communications from being intercepted. There is also the evidentiary issue of whether or not someone has tampered with the intercepted information. It may also be necessary to prevent technicians operating the communication system from accessing or viewing the intercepted information.

2

The invention addresses these and other problems with the present technology.

SUMMARY OF THE INVENTION

An intercept system provides more effective and more efficient compliance with legal intercept warrants. The intercept system can provide any combination of operations that include near-real-time intercept, capture of intercepted data in structured authenticated form, clear text intercept for communications where there is access to encryption keys, cipher text intercept for communications where there is no access to encryption keys, provision of transactional logs to the authorized agency, interception without altering the operation of the target services, and encryption of stored intercepted information.

The foregoing and other objects, features and advantages of the invention will become more readily apparent from the following detailed description of a preferred embodiment of the invention which proceeds with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a communication management system that operates a legal intercept system.

FIG. 2 is a diagram of an example log file generated for intercepted data.

FIG. 3 is a flow diagram showing in more detail how the log files in FIG. 2 are generated.

FIG. 4 is another block diagram showing how the legal intercept system operates with different types of encryption.

FIG. 5 is a diagram showing how intercepted data with different encryptions is converted into a log file.

FIG. 6 is a flow diagram showing in more detail how different types of encrypted data are formatted into a log file.

FIG. 7 is a diagram showing how a common transport is used for sending encrypted data.

FIG. 8 is a block diagram showing how an encryption schema in the communication management system is used in cooperation with the intercept system.

DETAILED DESCRIPTION

In the description below, an intercept event refers to an event where an agency issues a warrant requesting data interception for a targeted user. A targeted user is identified by a unique label, such as a username or account number, that corresponds to a user who is under intercept. A communication event, transaction, or intercept data is any message either sent or received by the targeted user. The intercept data can include synchronization messages, email data, calendars, contacts, tasks, notes, electronic documents, files or any other type of data passing through the communication management system.

Communication Management System

FIG. 1 shows an example of a communication network 12 that may operate similarly to the networks described in U.S. patent application Ser. No. 10/339,368 entitled: CONNECTION ARCHITECTURE FOR A MOBILE NETWORK, filed Jan. 8, 2003, and U.S. patent application Ser. No. 10/339, 368 entitled: SECURE, TRANSPORT FOR MOBILE COMMUNICATION NETWORK, filed Jan. 8, 2003, which are both herein incorporated by reference.

The communication system 12 in one implementation is used for intercepting data pursuant to legal search warrants. For example, a law enforcement agency may require the

operator of communication system 12 to intercept all messages sent to and from a mobile device 21. It should be understood that this is just one example of a communication system 12 and that the legal intercept system described in more detail below can operate with any communication network that is required to provide legal interception.

The communication system 12 includes a mobile network 14, an enterprise network 18, and a communication management system 16 that manages communications between the mobile network 14 and the enterprise network 18. The mobile 10 network 14 includes mobile devices 21 that communicate with an IP infrastructure through a wireless or landline service provider. Since mobile networks 14 are well known, they are not described in further detail.

The enterprise network 18 can be any business network, 15 individual user network, or local computer system that maintains local email or other data for one or more users. In the embodiment shown in FIG. 1, the enterprise network 18 includes an enterprise data source 34 that contains a user mailbox 44 accessible using a Personal Computer (PC) 38. In 20 one example, the enterprise data source 34 may be a Microsoft® Exchange® server and the PC 38 may access the mailbox 44 through a Microsoft® Outlook® software application. The mailbox 44 and data source 34 may contain emails, contact lists, calendars, tasks, notes, files, or any other 25 type of data or electronic document.

The PC **38** is connected to the server **34** over a Local Area Network (LAN) 35. The PC 38 includes memory (not shown) for storing local files that may include personal email data as well as any other types of electronic documents. Personal 30 the clear. client software 40 is executed by a processor 37 in the PC 38. The personal client 40 enables the mobile device 21 to access email, calendars, and contact information as well as local files in enterprise network 18 associated with PC 38.

or more management servers 28 that each include a processor 33. The processor 33 operates a transfer agent 31 that manages the transactions between the mobile device 21 and the enterprise network 18. A user database 42 includes configuration information for different users of the mobile communication service. For example, the user database 42 may include login data for mobile device 21.

While referred to as a communication management system 16 and management server 28, this can be any intermediary system that includes one or more intermediary servers that 45 operate between the mobile network 14 and the enterprise or private network 18. For example, a separate Smart Device Server (SDS) 30 may be used in management system 16 for handling communications with mobile devices in mobile network 14. Correspondingly, a SEVEN Connection Server 50 (SCS) 32 may be used for handling communications with personal clients in enterprise networks 18. Legal Interception

A Legal Intercept (LI) software module **50** is operated by the processor 33 and communicates with the transfer agent 31 55 Data Delivery in order to capture intercept data 49 associated with targeted user 51B. An operator sets up a configuration file 51 that is then used by the legal intercept module to automatically intercept communications for a particular target user and then format the intercepted communications into self authenticat- 60 ing log files.

An operator runs a toolkit utility 54 from a computer terminal 52 to configure the management server 28 for capturing intercept data 49. The toolkit utility 54 is used for creating and loading the configuration file 51 into memory in management 65 server 28 and can also display detected intercept data 49. To initiate an intercept, an entry is loaded into the configuration

file 51. To stop capturing intercept data 49, the system administrator deletes the entry or configuration file 51 from memory. Changes to the configuration file **51** of management server 28 may be automatically replicated to other management servers that are part of the communication management system 16. The toolkit utility 54 may have tightly controlled access that only allows operation by a user with an authorized login and password.

The toolkit **54** allows the operator to view, add, modify, and delete a warrant sequence number 51A, user identifier (ID) **51**B, and encryption key **57** in the configuration file **51**. The warrant identifier may be the actual sequence number for a wiretap or search warrant issued by a court of law and presented to the operator of communication management system 16 by a federal, state, or municipal government agency. The user ID **51**B for example may be an identifier used by communication management system 16 to uniquely identify different mobile clients 21.

The public encryption key 57 may be the public key component of a public/private key pair, such as a Pretty Good Privacy (PGP) or GNU Privacy Guard (GPG) public key, for encrypting the intercept data 49. In one embodiment, the legal intercept module 50 may not allow the management server 28 to start an interception process until a valid public key 57 is loaded into configuration file 51. This ensures that the intercepted data 49 can be immediately encrypted while being formatted into a log file **56**. If this encryption fails for any reason, the legal intercept module 50 may shut down the intercept process ensuring that no intercept data 49 is stored in

The configuration file **51** may also include one or more entries defining a transport protocol, destination, and associated configuration values for the transmission of intercepted data via a network. In one embodiment, this could include a The communication management system 16 includes one 35 destination email address associated with a Simple Mail Transfer Protocol (SMTP) host and port number or other Internet Protocol (IP) destination address that is used by the legal intercept module 50 to automatically transmit the intercept data 49 to mail box 77 on a remote server 76 that is accessible by the agency issuing the warrant.

After the configuration file **51** is enabled, the legal intercept module 51 starts intercepting data 49 associated with the targeted user identified by user ID 51B. As mentioned above, this can include any emails, calendar information, contacts, tasks, notes, electronic documents, files or any other type of control or content data associated with user ID 51B. The intercepted data can include any type of communications such as email sent or received, calendar items sent or received, and other data sent/received by and from the targeted smart device 21. The captured intercept data 49 may then be encrypted using the encryption key 57 contained in the configuration file **51**. The encrypted copy of the captured intercept data 49 may then be formatted and written to log file **56**.

The legal intercept module 50 running on each management server 28 may periodically poll the directory or location containing the encrypted intercept log files 56 for each user ID under intercept for the presence of new files or data. The poll period in one example is approximately every minute. Of course this is only one example and any user configurable time period can be used. New intercept data 49 which has been stored in one or more log files 56 and identified by the legal intercept module 50 during the polling process may be automatically reprocessed and/or transmitted according to the specification in configuration file **51**. As an alternative to storing encrypted intercept data 49 in log file 56 on a file

system, intercept data may be stored in database 42. Also, as shown in FIG. 4, the log file 56 may be stored in an alternative file system 53 located within the management server 28. The agency issuing the warrant can then access the data contained in log files 56 or database 42 in one of many different ways.

In one implementation, an official from the agency physically sits at terminal **52** at the location of communication management system **16**. The agency official then reads the log files **56** in semi-real-time as the intercept events **49** are being detected in the management server **49**. The agency official then uses terminal **52** to store or copy the log files **56** onto a portable storage medium, such as a Compact Disc (CD), memory stick, etc. In this implementation, the legal intercept log files **56** may not reside in user database **42** at all, or may only reside in database **42** for some relatively brief period of time while being transferred onto the portable storage media.

A copy of the log files may be stored onto the portable storage medium while the same log files remain in the communication management system 16. The copy of the log files 20 in the management system 16 could then be used, if necessary, for evidentiary purposes when admitting the copy under control of the agency official into evidence.

In an alternative implementation, the legal intercept module **50** may automatically send the log files **56** for the intercepted events to an email mailbox **77** operated in a remote server **76**. The remote server **76** may be located in a wireless service provider network or may be located at the facilities of the enforcement agency issuing the warrant. In this implementation, a terminal **72** at the remote location **70** may include a toolkit utility **54** that has some of the same functionality as toolkit **54**. The utility **54** only allows authorized users to decrypt and access the log files **56** received from communication management system **16**.

For example, the toolkit utility **54** may include public and private PGP or GPG encryption keys **57** and **55**, respectively, that are associated with the public encryption key **57** previously loaded into configuration file **51**. Only personnel having authorized access to the toolkit **54** can decrypt and read the log files **56** previously generated and encrypted by legal intercept module **50**. This provides additional privacy of the intercept data **49** from technical personnel of the communication management system **16** that may not be authorized to view the intercept data **49**.

The intercept module **50** may transfer each captured log file **56** to a SMTP email server **76** via the Simple Mail Transfer Protocol (SMTP). The SMTP server **76** stores each log file **56** in an inbox of mailbox **77**. The name of the mailbox **77** may be the same as the warrant sequence number @ the 50 agency's domain name. For example, warrant123@LAPD. com. The warrant sequence number may correspond with the warrant identifier **51**A in configuration file **51** and the domain name may correspond with the IP address **51**D in configuration file **51**. Once transmitted and accepted by the SMTP 55 email server **76**, the log file **56** may be automatically deleted from user database **42**.

The agency issuing the warrant can retrieve the captured log files **56** in remote server **76** for a particular user ID under interception using for example the Post Office Protocol 60 (POPv3). The agency is given the name of email server **76**, POP and SMTP port numbers, the mailbox id (warrant sequence number **51**) and a password to access the mailbox **77**. The agency then retrieves log files **56** in mailbox **77** using POP. Once a file is downloaded from the mailbox **77** to an 65 agency terminal **72**, the log file **56** may be automatically deleted from the mailbox **77**.

6

Log Files

Referring to FIGS. 1 and 2, the legal intercept software 50 generates log files 56 in a structured manner that provides more secure and reliable data authentication. In this example, an intercept directory 60 is loaded with log files 56 generated to account for every minute of a particular time period, such as an entire day. The legal intercept 50 may generate a name for directory 60 that identifies the contents as legal intercepts, for a particular user ID and for a particular day. Of course this is just one naming convention that can be used to more efficiently organize log files.

The log files **56** stored in directory **60** may indicate the number of events intercepted for the targeted device during each minute. For example, a first log file **56**A is identified by the following log file name: fe0-2005/09/23-00:00.ASC, containing a single line that reads as follows: "0 events logged in the last minute". This indicates that a management server fe0 on Sep. 23, 2005, at 12:00 midnight logged zero intercept events for a particular user ID during the specified time period. A second log file **56**B is named to identify a next minute of the intercept period and indicates that between 12:00 A.M and 12:01 A.M, on the same day, no intercept events were logged.

The first detected intercept events for this particular user ID for this particular day were detected in log file **56**C identified by the log file name: fe0-2005/09/23-00:02.ASC, the first and/or last line of which reads "3 events logged in the last minute". Log file **56**C indicates that 3 intercept events were detected on Sep. 23, 2005, between 12:01 A.M. and 12:02 A.M. The legal intercept **50** generates this contiguous set of log files **56** that cover each minute or other configured interval of the intercept period.

The legal intercept 50 may also load a first entry into the log file directory 60 that lists the warrant id 51A, PGP key 57, etc. The legal intercept 50 may also generate a log file 56 that indicates any management server status-change events. For example, if the management server 28 conducts a graceful shutdown, a log file 56 may be generated that indicates when the shut down occurred and possibly the cause of the shutdown.

This highly structured log file format provides the agency official a quick indicator of when intercept events are detected for a particular target user. Further, as shown above, the log files are created contiguously for predetermined time periods over a particular intercept period even when no intercept events are detected. This provides further verification that the legal intercept 50 was actually in operation and continuously monitoring for intercept events during the intercept period.

As described above, the log files **56** may be stored into a portable storage media that can be transported by an agency official. Alternatively, the log files **56** may be stored in the user database **42** in the communication management system **16** for later retrieval by the agency official via toolkit **54**. In another implementation, the log files **56** may be sent to the mailbox **77** in a server **76** in a mobile operator infrastructure which is accessible by the agency official.

FIG. 3 explains in further detail how the legal intercept module 50 might generate the log files. In operation 61, communications are monitored for a particular targeted user for predetermined time periods over an intercept period. In one example as described above, the predetermined time period may be one minute. Of course, time periods of less than one minute or more than one minute may also be used. The duration of these time periods may also be configurable by setting a parameter in configuration file 51. If no intercept

events are detected during the predetermined time period in operation 62, an empty log file is generated for that time period in operation 63.

When intercept events are detected, all the intercepted data for that time period is formatted into a same log file **56** in 5 operation **64**. The log file is encrypted in operation **65** using the encryption key **57** (FIG. **1**) loaded by the toolkit **54** into configuration file **51**. All of the encrypted log files **56** associated with a particular targeted user for a particular intercept period are stored in a same intercept directory **60** (FIG. **2**). For example, all log files generated for a particular user ID for a same day are stored in the same intercept directory. If the current day of legal interception is not completed in operation **66**, further monitoring and interception is performed in operation **61**.

When interception for a current interception period is completed, a Cyclic Redundancy Check (CRC) value, or some other type of digital certificate/signature, may be generated in operation 67. The CRC can be used to verify that the contents of intercept directory 60 have not been tampered with or 20 deleted after their initial generation. The CRC may be encrypted in operation 68 and then separately emailed to the agency or separately stored for later validation. As discussed above, the encrypted log files may then either be emailed to a mailbox or stored locally for later retrieval by the enforcement agency.

Thus, the individual log file encryption in operation **65** ensures the authenticity of intercepted events for a particular time period and the CRC generated in operation **67** ensures that none of the individual log files have been removed or ³⁰ replaced.

Encrypted Intercept Data

Referring to FIG. 4, as described above, the log files 56 may be stored in database 42 or in a file system 53 within the management server 28. A single or multi-tiered encryption 35 scheme may be used in network 12. For example, the personal client 40 may make an outbound connection 25 to the management server 28. The personal client 40 registers the presence of a particular user to the management server 28 and negotiates a security association specifying a cryptographic 40 ciphersuite (including encryption cipher, key length, and digital signature algorithm) and a unique, secret point-topoint encryption key 29 over connection 25. In one example, the key 29 is an Advanced Encryption Standard (AES) key. Of course, encryption ciphers other than AES can also be used. 45 The encryption key 29 enables secure communication between management server 28 and PC 38 over connection **25**.

The mobile device 21 also negotiates a point-to-point security association, specifying a cryptographic ciphersuite and a unique encryption key 27, with the management server 28. In one example, the point-to-point encryption key 27 is also an AES encryption key. The negotiated security association that includes encryption key 27 enables secure point-to-point communication between the mobile device 21 and the management server 28 over connection 23. Each different mobile device 21 negotiates a different security association that includes a unique encryption key 27 with the management server 28.

The point-to-point encryption key 27 may be used for 60 encrypting control data that needs to be transferred between the mobile device 21 and management server 28. The point-to-point encryption key 29 may be used for encrypting control data that needs to be transferred between the management server 28 and personal client 40. For example, the control data 65 may include login information and transaction routing information.

8

An end-to-end security association, specifying a cryptographic ciphersuite and a unique encryption key 46, is negotiated between the mobile device 21 and the personal client 40. In one example, the end-to-end encryption key 46 is also an AES encryption key. The end-to-end encryption key 46 in one example is used for encrypting transaction payloads transferred between personal client 40 and mobile device 21. For example, the end-to-end encryption key 46 may be used for encrypting the content of emails, files, file path names, contacts, notes, calendars, electronic documents and any other type of data transferred between mobile device and the PC. The end-to-end encryption key 46 is only known by the mobile device 21 and the personal client 40. Data encrypted using the end-to-end key 46 cannot be decrypted by the management server 28.

Referring to FIGS. 4 and 5, the legal intercept module 50 can produce log files 56 from intercept data 49 that have any combination of unencrypted data 49A sent in the clear, point-to-point encrypted data 49B encrypted using the point-to-point encryption keys 27 or 29, and end-to-end encrypted data 49C encrypted using the end-to-end encryption key 46.

The communication management system 16 has access to the point-to-point encryption keys 27 and 29 used for encrypting the point-to-point encrypted information 49B. Therefore, the management system 16 can automatically decrypt the point-to-point encrypted information 49B before it is reformatted into log file 56.

The end-to-end encryption keys 46 are only shared between the endpoints 21 and 38 and are unknown to the communication management system 16. Therefore, the agency issuing the warrant may be required to extract the end-to-end encryption keys 46 either at the mobile device 21 or at the enterprise server 34 or personal computer 38. The end-to-end encrypted information 49C may then be decrypted at a later time separately from the point-to-point encrypted information 49B.

For example, after receiving and decrypting the log file 56, the enforcement agency may then independently conduct a seizure of the end-to-end encryption key 46 from either the enterprise network 18 or the mobile device 21. The enforcement agency could then separately decrypt information 56B in log file 56 with the seized end-to-end encryption key 46.

FIG. 6 explains in more detail how the legal intercept module 50 handles the decryption and reformatting of intercept data into log files. In operation 80, the management server 28 is configured to conduct a legal intercept for a particular user ID as described above in FIG. 1. Accordingly, the management server 28 begins intercepting data for the identified user ID in operation 82.

In operation 84, any point-to-point encrypted portion 49B of the intercepted data 49 (FIG. 5) is decrypted. In operation 86, the decrypted point-to-point data is combined with any information 49A in the intercept data 49 received in the clear. The unencrypted data is then formatted into an unencrypted portion 56A of the log file 56 in FIG. 5. Any end-to-end encrypted data 49C is then combined in the same log file 56 as section 56B in operation 88. The log file 56 is then possibly encrypted in operation 90 and then either stored in a local database or automatically sent to a remote server.

Detecting Different Types of Intercept Data

FIGS. 7 and 8 explain in more detail how a particular data format used by the communication system 12 can be used to identify point-to-point and end-to-end encrypted intercept data. FIG. 7 shows how encryption can be performed differently for different types of data or for data associated with different destinations. Intercept data 102 includes content data 108 such as the contents of an email message, an elec-

tronic document, or any other type of information that should only be accessed by two endpoints. The content data 108 in this example is encrypted using an end-to-end encryption key.

A second portion 106 of intercept data 102 may include control information that only needs to be processed by one particular server. In this case, control data 106 may be encrypted using a first point-to-point encryption key. A third portion 104 of intercept data 102 may have other control information, for example, error checking data, that needs to be processed by a different server. Accordingly, the error checking data 104 is encrypted using a second point-to-point encryption key different than either of the other two encryption keys used for encrypting data 108 and 106.

FIG. 8 shows in more detail an encryption schema 112 is used by the mobile device 21, management server 28, and personal client 40 when processing transactions between a source and a target device. In the example below, the mobile device 21 is operating as a source for sending a transaction 110. The transaction 110 requests personal client 40 to send a document 114 located in a personal directory in local memory 116 of PC 38. The personal client 40 operates as a target for the transaction 110 and the management server 28 operates as the transfer agent for transferring the transaction 110 from the mobile device 21 to the personal client 40.

It should be understood that this is only an example, and the devices shown in FIG. 8 can process many different types of transactions. For example, the transaction 110 may request synchronization of emails in the PC 38 with emails in the mobile device 21. Further, any device can operate as a source or target for the transaction. For example, the personal client 40 operates as a source and the mobile device 21 operates as a target when a transaction 111 is sent as a reply to request 110.

The mobile device 21, management server 28, and the personal client 40 are all configured with an encryption schema 112 that identifies how specific items in the transaction 110 are to be encrypted. Each device is also configured with different security associations as described above in Point (PP) key 27 and End-to-End (EE) key 46. Management server 28 has PP key 27 and PP key 29, and the PC 38 has PP key 29 and EE key 46.

The channel cont monly known as server referred to as data group partition, group, etc.

The channel cont monly known as server 28 to as data group partition, group, etc.

The channel cont monly known as server 28 to as data group partition, group, etc.

The channel cont monly known as server 28 to as data group partition, group, etc.

The contents of the of bits referred to as channel are encoded group 2, and the contents of the

The mobile device **21** forms the request transaction **110**. 45 One example of a request is as follows.

```
Request: {auth_token = "abc",
device_id = "xyz",
method_id = "GetDocument",
args = {path = "/docs"}
}
```

Mobile device 21 attaches an auth_token to transactions sent to the management server 28. For example, the mobile device 21 may be required to authenticate to the management server 28 by transmitting a username and password prior to being permitted to submit other transactions for processing. The management server 28 issues the mobile device 21 an auth_token after successfully validating the username and password against information in the user database 42. The mobile device 21 then attaches the auth_token to subsequent transactions sent to the management server 28. The management server 28 uses the auth_token to identify and authenticate the source of each transaction and to determine where to route the transaction.

10

The device_id identifies the particular mobile device 21 sending the request 110. The device_id may be necessary, for example, when a user has more than one mobile device. The personal client 40 can use different device_id values to track when synchronization information was last sent to each of multiple different mobile devices. The device_id can also be used by either the management server 28 or the personal client 40 to determine how to format data sent to particular types of mobile devices 21. For example, data may need to be formatted differently for a cell phone as opposed to a personal computer. The device_id can also be used to correlate a known security association with a particular mobile device.

The method_id item in the example identifies a particular function GetDocument associated with request 110. The method_id item also requires the inclusion of related argument items that identify the parameters for the GetDocument function. For example, the argument items might include the expression path="/docs" identifying the pathname where the requested documents are located.

In order to prepare the request 110 for transmission, the mobile device 21 performs a pattern match of the request 110 using the encryption schema 112. This pattern match separates the items in request 110 into different channels. One example of the different channels is shown below. In this example, the items in each channel are associated with predefined security associations: clear, pp, and ee.

The channel contents are encoded (via a process commonly known as serialization) into arrays of bits or bytes referred to as data groups. These groupings of bits or bytes are referred to generally below as arrays, but can be any type of partition, group, etc.

The contents of the clear channel are encoded into an array of bits referred to as data_group_1, the contents of the pp channel are encoded into an array of bits referred to as data_group_2, and the contents of the ee channel are encoded into an array of bits referred to as data_group_3. The contents of each channel need to be encoded into bit arrays so that they can be encrypted. The contents of the channels after being encoded into bit arrays are represented as follows.

```
Encoded
Channels: {clear = data_group_1
pp = data_group_2
ee = data_group_3 }
```

The bit arrays are then encrypted according to the security association parameters for each channel. According to the encryption schema 112, bits in the clear channel (data_group_1) are not encrypted. The bits in the pp channel data_group_2 are encrypted using the point-to-point security association between mobile device 21 and management server 28, using PP key 27, and are referred to after encryption as pp_data_group_2. The bits in the ee channel data_group_3 are encrypted using the end-to-end security association between mobile device 21 and personal client 40, using EE key 46, and are referred to after encryption as ee_data_group_3. The data groups are represented as follows after encryption:

11

Encrypted	
Channels:	{clear = data_group_1
	pp = pp_data_group_2
	ee = ee_data_group_3}

The bits making up the encrypted and unencrypted channels are then encoded into one or more packets. For clarity, the description below will refer to a single packet, however, the data from the channels may be contained in multiple packets. 10 Some of the contents of the packet are shown below.

	Packet:
Header	length version flags
Payload	count = 3 "clear" data_group_1 pp_data_group_2 "ee" ee_data_group_3

Information in the packet header may include the packet length, a version number, and other flags. The packet payload includes a count identifying 3 pairs of items. The three items include the non-encrypted contents in the clear channel, the pp encrypted contents of the pp channel, and the ee encrypted contents of the ee channel. The packet is then transported by mobile device **21** to the management server **28**.

The transfer agent operating in server **28** receives the packet. The bits in the packet are separated into the different channels clear=data_group_1, pp=pp_data_group_2, and ee=ee_data_group_3.

The data in the clear channel does not need to be decrypted. The transfer agent decrypts the only bits in channels for which it has a known security association. The transfer agent, as a member of the point-to-point security association between mobile device 21 and management server 28, possesses the PP key 27 and therefore decrypts the contents of the pp 40 channel. The transfer agent is not a member of the end-to-end security association between mobile device 21 and personal client 40, does not have the EE key 46 and therefore does not decrypt the data in the ee channel. Decryption produces the clear data_group_1, following data groups: pp=data_group_2, and ee=ee_data_group_3.

The transfer agent decodes the contents of the clear and pp channels. The contents of the encrypted ee channel are not decoded, but instead are maintained in an unmodified state for eventual transport to the personal client **40**. Decoding produces the following contents.

```
Decoded
Channels: {clear = {device_id = "xyz"} }
pp = {auth_token = "abc", method_id = "GetDocument"} ee=ee_data_group_3 }
```

A partial request is formed by merging the items of the clear and pp channels. The partial request in this example could look similar to the following:

```
Partial Request: {auth_token = "abc",
device_id = "xyz",
method_id = "GetDocument",
```

12

```
-continued
```

```
args = { }
encrypted = {ee=ee_data_group_3}
}
```

The transfer agent 31 in the management server 28 processes the partial request. In this example, the transfer agent may verify the request is authorized by matching the value of auth_token ("abc") with contents in the user database 42 (FIG. 8). The auth_token and the method_id ("GetDocument") indicate that the transaction 110 is a document request directed to the personal client 40.

The transfer agent may identify a user_id="joe" associated with the auth_token="abc" and generate the following new request.

```
New Request: {user_id = "joe",
device_id = "xyz",
method_id = "GetDocument",
args = { }
encrypted = {ee=ee_data_group_3}
}
```

The legal intercept 50 in FIG. 1 may come into play at this point, or earlier in the encryption schema 112. For example, the legal intercept 50 checks the user_id in the request with the user id 51B in the intercept configuration file 51. In this example, if "joe" matches the user_id 51B in configuration file 51, then the contents in the request are formatted into a log file 56 as described above. As can be seen, at this point the new request has already decrypted the auth_token="abc" and method_id="GetDocument". Further, the device_id="xyz" was received in the clear. The legal intercept 50 simply has to format these different channels into a log file.

The end-to-end encrypted data in group 3 remains encrypted and therefore may not provide all of the information desired for the enforcement agency. However, the decrypted information does provide enough information to adequately indicate that the intercepted data is associated with a particular user_id. The intercepted unencrypted data may also provide further evidence that the enforcement agency can then use to obtain another warrant to seize the ee encryption key from the targeted user.

As described above in FIG. 2, the legal intercept 50 may then attach appropriate time/date stamp headers to this raw data frame to authenticate the time and date when the data was intercepted.

End-to-End Encrypted Data

As described above, the communication management system 16 may not have access to the end-to-end encryption keys 46 (FIG. 2). However, as shown in FIG. 8, the management server 28 is still capable of identifying data streams belonging to users targeted for interception, as this identifying information is required for routing the datagrams shown above. Thus, the legal intercept module 50 can still intercept data that cannot be immediately decrypted.

The intercept logs **56** can therefore contain data encrypted using encryption keys known only to the endpoints. For example, a mobile device **21** and a desktop connector running on personal computer **38** (FIG. **1**). The toolkit **54** in FIG. **1** can facilitate the recovery of the end-to-end keys **46**.

In order to make use of this functionality, the enforcement agency seeking the information may need to obtain both an intercept warrant, and either a search-and-seizure warrant authorizing the extraction of the configuration data from the

smart device client in the mobile device 21 or a search-and-seizure warrant authorizing the extraction of the end-to-end encryption key from the desktop connector in the PC 38 (FIG. 1).

After the authorized agency has executed the necessary 5 warrants, the toolkit 54 is used by the agency to facilitate the recovery of the end-to-end key 46. The toolkit utility 54 then uses the end-to-end key 46 to decrypt the end-to-end encrypted information in the log files 56.

The system described above can use dedicated processor 10 systems, micro controllers, programmable logic devices, or microprocessors that perform some or all of the operations. Some of the operations described above may be implemented in software and other operations may be implemented in hardware.

For the sake of convenience, the operations are described as various interconnected functional blocks or distinct software modules. This is not necessary, however, and there may be cases where these functional blocks or modules are equivalently aggregated into a single logic device, program or operation with unclear boundaries. In any event, the functional blocks and software modules or features of the flexible interface can be implemented by themselves, or in combination with other operations in either hardware or software.

Having described and illustrated the principles of the 25 invention in a preferred embodiment thereof, it should be apparent that the invention may be modified in arrangement and detail without departing from such principles. Claim is made to all modifications and variation coming within the spirit and scope of the following claims.

The invention claimed is:

- 1. A method for intercepting data, comprising:
- receiving, at a management server, a connection from a remote client, the connection being initiated by the 35 remote client and established outbound from the remote client;
- negotiating a point-to-point encryption scheme with a remote mobile device, the point-to-point encryption scheme negotiated between the management server and 40 the remote mobile device;
- receiving, at the management server, a value identifying an intercept target for a legal intercept and an indication that interception is authorized by a warrant, the intercept target corresponding to the remote mobile device;
- automatically intercepting, at the management server, data received and/or sent by the intercept target identified by the value, wherein data is intercepted without altering operation of email application services that operate on the remote mobile device;
- inspecting packets having the intercepted data to distinguish end-to-end encrypted information from other information that is encrypted according to the point-to-point encryption scheme negotiated with the remote mobile device;
- preserving encryption that is included on the end-to-end encrypted information when received while removing encryption that is included on at least a portion of the other information, said other information decrypted using a key obtained during the point-to-point encryp- 60 tion scheme negotiation; and
- transferring both the decrypted other information and the end-to-end information from the management server to a remote device.
- 2. The method of claim 1, wherein the packets are intercepted during a requested time period, and the method further comprises:

14

- formatting the data that is intercepted during the requested time period and associated with the target user into one or more first log files, each of the first log files corresponding to a different time segment occurring during the requested time period and indicating one or more intercept events for its corresponding time segment; and
- formatting one or more second different log files associated with the requested time period, the second log files indicating inactivity and corresponding to different remaining time segments that occur during the requested time period and that are unrepresented by the first log files that indicate the intercept events such that the first and second log files record monitoring for the entire requested time period independently of whether the data is intercepted intermittently during the requested time period.
- 3. The method of claim 2, wherein the data is intercepted according to an intercept configuration file that includes at least a unique intercept identifier and a user ID identifying the target user.
- 4. The method of claim 2, wherein the log files record an unbroken sequence of continuous monitoring over the requested time period independently of whether the data is intercepted intermittently.
- 5. The method of claim 2, further comprising transferring the log files to the remote device.
- 6. The method of claim 2, further comprising formatting the log files with different time values usable for verifying that communications from the remote mobile device were continuously monitored during the requested time period regardless of whether the data was intercepted intermittently.
- 7. The method according to claim 1, wherein the encryption that is included on the end-to-end encrypted information uses a security association that is kept secret from the management server such that the end-to-end encrypted information is kept private with respect to employees associated with the management server.
- 8. The method of claim 1, further comprising determining whether to encrypt at least one of the end-to-end information and the decrypted information prior to said transferring.
 - 9. The method according to claim 1, further comprising: combining, at the management server, the end-to-end encrypted information of the intercepted data with the decrypted other information of the intercepted data in a same log file.
 - 10. The method according to claim 1, further comprising: storing, at the management server, the intercepted data in a structure format that identifies when the data was intercepted and at the same time provides authentication that the stored intercepted data has not been altered or deleted.
- 11. The method according to claim 10, further comprising monitoring communications between the remote client and the remote mobile device for multiple contiguous time periods.
 - 12. The method according to claim 11, further comprising: generating, using the management server, log files over an intercept period that encompasses the multiple contiguous time periods;
 - storing the log files in a same intercept directory;
 - inserting a warrant identifier received together with the value into the intercept directory; and
 - generating a name for the intercept directory that identifies the intercept target and the intercept period over which the log files were generated.

- 13. The method according to claim 12, further comprising: encrypting the log files in the intercept directory with an encryption scheme known by an agency issuing the warrant, said encryption performed using the management server that intercepted the data; and
- sending the encrypted intercept directory to an electronic mailbox accessible by the agency.
- 14. The method according to claim 13, further comprising: generating a Cyclic Redundancy Check (CRC) or other digital signature value for all of the log files in the 10 intercept directory;

encrypting the resulting generated value; and

- providing the encrypted generated value to the enforcement agency, said encrypted generated value sent in a different communication than the encrypted intercept directory, said encrypted generated value verifying that the log files have not been altered.
- 15. The method according to claim 1, further comprising: reading an intercept configuration file that contains a warrant identifier, the value identifying the user, an enforcement 20 agency known encryption key and an electronic mailbox address;
 - upon reading the intercept configuration file automatically intercepting data received and/or sent by the remote mobile device;
 - formatting any intercepted data into log files that identify when the data was intercepted; and

encrypting the log files using the encryption key.

- 16. The method according to claim 1, wherein the end-to-end encrypted information is associated with content and is 30 protected with an end-to-end encryption scheme that is kept secret from any midpoints located on a call path between transmitting and receiving endpoints, and the other information is associated with transaction routing information and is protected with the negotiated point-to-point encryption 35 scheme.
 - 17. A communication management system, comprising: a management server configured to receive a connection initiated by a remote client and established outbound from the remote client;
 - the management server configured to negotiate a point-topoint encryption scheme with a remote mobile device, the point-to-point encryption scheme negotiated between the management server and the remote mobile device;
 - the management server configured to receive a value identifying an intercept target for a legal intercept and an indication that interception is authorized by a warrant, the intercept target corresponding to the remote mobile device;
 - the management server configured to automatically intercept data received and/or sent by the intercept target identified by the value, wherein the data is intercepted without altering operation of email application services that operate on the remote mobile device;
 - the management server configured to inspect packets having the intercepted data to distinguish end-to-end encrypted information from other information that is encrypted according to the point-to-point encryption scheme negotiated with the remote mobile device;
 - the management server configured to preserve encryption that is included on the end-to-end encrypted information when received while removing encryption that is included on at least a portion of the other information, said other information decrypted using a key obtained 65 during the point-to-point encryption scheme negotiation; and

16

- the management server configured to transfer both the decrypted other information and the end-to-end information from the management server to a remote device.
- 18. The communication management system of claim 17, further comprising:
 - the management server configured to automatically format the intercepted data into log files;
 - the management server configured to generate multiple log files that identify any intercepted data for associated contiguous predetermined time periods extending over a continuous intercept period; and
 - the management server configured to generate the log files for back-to-back time periods, the management server further configured to generate each log file by selecting between inserting the intercepted data and an inactivity indication therein such that each of the log files contains at least one selected from the group comprising the intercepted data for the associated time period and an indication that no data was intercepted during the associated time period.
- 19. The communication management system of claim 18, further comprising:
 - the management server is configured to select a same duration for the time periods according to selectable time interval values included in an intercept configuration file.
- 20. The communication management system of claim 18, further comprising:
 - the management server configured to encrypt the log files according to an encryption key known by an enforcement agency associated with the warrant before emailing the encrypted log files to a mailbox for the enforcement agency.
- 21. The communication management system of claim 18, further comprising:
 - the management server configured to identify a first portion of the intercepted data encrypted using a first known security association for which the management server has knowledge of the encryption key and identify a second portion of the intercepted data encrypted using a second unknown security association, the management server configured to decrypt and store the first portion of the intercepted data into an associated one of the log files and combine the encrypted second portion of the intercepted data with the decrypted first portion of the intercepted data in the same associated log file.
- 22. The communication management system of claim 21, wherein the first portion of the intercepted data is encrypted with a known point-to-point encryption key and the second portion of the intercepted data is encrypted with an unknown end-to-end encryption key.
 - 23. The communication management system of claim 21, further comprising:
 - the management server is configured to encrypt both the decrypted first portion of the intercepted data and the second encrypted portion of the intercepted data.
- 24. The communication management system of claim 21, wherein the first portion of the intercepted data includes transaction authentication and routing information and the second portion of the intercepted data includes the contents of email messages, electronic files, or other electronic data.
 - 25. The communication management system of claim 17, wherein the management server is configured to process communications exchanged between a local device operating in an enterprise or local network and a mobile wireless device that synchronizes with a portion of the data in the local device.

26. A method for intercepting data, comprising:

in response to receiving a connection request, negotiating a point-to-point encryption scheme with a mobile device, the point-to-point encryption scheme negotiated between a management server and the mobile device;

automatically intercepting, at the management server, data received and/or sent by an intercept target, wherein data is intercepted without altering operation of application services on the mobile device;

inspecting packets having the intercepted data to distinguish end-to-end encrypted information from other information that is encrypted according to the point-topoint encryption scheme negotiated with the device;

preserving encryption that is included on the end-to-end encrypted information when received while removing encryption that is included on at least a portion of the other information, said other information decrypted using a key obtained during the point-to-point encryption scheme negotiation; and

transferring both the decrypted other information and the end-to-end information.

27. The method of claim 26, further comprising, receiving, at the management server, a value identifying the intercept target for a legal intercept and an indication that interception 25 is authorized by a warrant, the intercept target corresponding to the mobile device.

28. The method of claim 26, wherein the packets are intercepted during a requested time period, and the method further comprises: formatting the data that is intercepted during the 30 requested time period and associated with a target user into one or more first log files.

29. The method of claim 28, wherein: each of the first log files corresponding to a different time segment occurring during the requested time period and indicating one or more 35 intercept events for its corresponding time segment.

30. The method of claim 29, further comprising:

formatting one or more second different log files associated with the requested time period, the second log files indicating inactivity and corresponding to different remain- 40 ing time segments that occur during the requested time period and that are unrepresented by the first log files that indicate the intercept events such that the first and second log files record monitoring for the entire requested time period independently of whether the data 45 is intercepted intermittently during the requested time period.

31. The method of claim 28, wherein the log files record an unbroken sequence of continuous monitoring over the requested time period independently of whether the data is 50 intercepted intermittently.

32. The method of claim 28, further comprising formatting the log files with different time values usable for verifying that communications from the mobile device were continuously monitored during the requested time period regardless of 55 whether the data was intercepted intermittently.

33. The method of claim 26, wherein the data is intercepted according to an intercept configuration file that includes at least a intercept identifier and a user ID identifying a target user.

34. The method of claim 26, wherein the encryption that is included on the end-to-end encryption information uses a security association that is kept secret from the management.

35. The method of claim 26, further comprising determining whether to encrypt at least one of the end-to-end infor- 65 mation and the decrypted information prior to said transferring.

18

36. The method according to claim 26, further comprising: combining the end-to-end encrypted information of the intercepted data with the decrypted other information of the intercepted data in a log file.

37. The method according to claim 26, further comprising: storing the intercepted data in a structure format that identifies when the data was intercepted and provides authentication that the stored intercepted data has not been altered or deleted.

38. The method according to claim 26, further comprising monitoring communications between a remote client and the device for multiple contiguous time periods.

39. The method according to claim 38, further comprising: generating log files over an intercept period that encompasses the multiple contiguous time periods;

storing the log files in a same intercept directory.

40. The method according to claim 39, further comprising: inserting a warrant identifier received together with the value into the intercept directory; and

generating a name for the intercept directory that identifies the intercept target and the intercept period over which the log files were generated.

41. The method according to claim 39, further comprising: encrypting the log files in the intercept directory with an encryption scheme known by an agency issuing the warrant, said encryption performed using the management server that intercepted the data; and

sending the encrypted intercept directory to an electronic mailbox accessible by the agency.

42. The method according to claim 39, further comprising: generating a Cyclic Redundancy Check (CRC) or other digital signature value for all of the log files in the intercept directory;

encrypting the resulting generated value; and

providing the encrypted generated value to the enforcement agency, said encrypted generated value sent in a different communication than the encrypted intercept directory, said encrypted generated value verifying that the log files have not been altered.

43. The method according to claim 26, further comprising: reading an intercept configuration file that contains a warrant identifier, the value identifying the user, an enforcement agency known encryption key and an electronic mailbox address;

upon reading the intercept configuration file automatically intercepting data received and/or sent by the remote mobile device;

formatting any intercepted data into log files that identify when the data was intercepted; and

encrypting the log files using the encryption key.

44. The method according to claim 26, wherein the end-toend encrypted information is associated with content and is protected with an end-to-end encryption scheme that is kept secret from any midpoints located between transmitting and receiving endpoints, and the other information is associated with transaction routing information and is protected with the point-to-point encryption scheme.

45. A communication management system for intercepting data, comprising:

a processor;

a network interface configured to receive a connection request; and

a memory unit having instructions stored thereon, wherein the instructions, when executed by the processor, causes the communication management system to: negotiate a point-to-point encryption scheme;

inspect packets having the data to be intercepted to distinguish end-to-end encrypted information from other information that is encrypted according to the point-to-point encryption scheme;

preserve encryption that is included on the encrypted information when received while removing encryption that is included on at least a portion of the other information, said other information decrypted using a key obtained in association with the point-to-point 10 encryption scheme;

transfer both the decrypted other information and the end-to-end encrypted information;

automatically format the intercepted data into log files including:

generating log files that identify intercepted data for associated contiguous predetermined time periods extending over a continuous intercept period; and generating the log files for back-to-back time periods, the management server generating each log file by selecting between inserting the intercepted data and an inactivity indication therein such that each of the log files contains at least one selected from the group including the intercepted data for the associated time period and an indication that no data was intercepted during the associated time period;

negotiate the point-to-point encryption scheme with a mobile device in response to receiving the connection request, and

intercept data received and/or sent by an intercept target, wherein data is intercepted without altering operation of application services on the mobile device.

* * * *