US007181017B1

(12) **United States Patent**
Nagel et al.

(10) **Patent No.: US 7,181,017 B1**
(45) **Date of Patent: Feb. 20, 2007**

(54) **SYSTEM AND METHOD FOR SECURE THREE-PARTY COMMUNICATIONS**

(75) Inventors: **Robert H. Nagel**, New York, NY (US); **David P. Felsher**, Trumbull, CT (US); **Steven M. Hoffberg**, West Harrison, NY (US)

(73) Assignee: **David Felsher**, Trumbull, CT (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 818 days.

(21) Appl. No.: **10/106,138**

(22) Filed: **Mar. 25, 2002**

Related U.S. Application Data

(60) Provisional application No. 60/278,317, filed on Mar. 23, 2001.

(51) **Int. Cl.**
H04L 9/00 (2006.01)

(52) **U.S. Cl.** **380/282**; 380/44

(58) **Field of Classification Search** ..... None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,200,770	A	4/1980	Hellman
4,218,582	A	8/1980	Hellman
4,264,782	A	4/1981	Konheim
4,306,111	A	12/1981	Lu
4,309,569	A	1/1982	Merkle
4,326,098	A	4/1982	Bouricius
4,351,982	A	9/1982	Miller
4,365,110	A	12/1982	Lee
4,386,233	A	5/1983	Smid
4,393,269	A	7/1983	Konheim
4,399,323	A	8/1983	Henry
4,405,829	A	9/1983	Rivest
4,438,824	A	3/1984	Mueller-Schloer
4,453,074	A	6/1984	Weinstein
4,458,109	A	7/1984	Mueller-Schloer
4,471,164	A	9/1984	Henry
4,514,592	A	4/1985	Miyaguchi
4,528,588	A	7/1985	Lofberg
4,529,870	A	7/1985	Chaum
4,558,176	A	12/1985	Arnold
4,564,018	A	1/1986	Hutchison
4,564,840	A *	1/1986	Brisse et al. 342/47

(Continued)

OTHER PUBLICATIONS

Matt Blaze et al., "Divertible Protocols and Atomic Proxy Cryptography", 1998. http://citeseer.ist.psu.edu/blaze98atomic.html.*

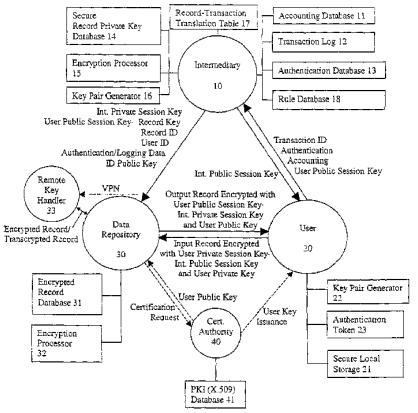
(Continued)

Primary Examiner—Gilberto Barrón, Jr.
Assistant Examiner—Virgil Herring
(74) *Attorney, Agent, or Firm*—Milde & Hoffberg LLP

(57) **ABSTRACT**

A system and method for communicating information between a first party and a second party, comprising identifying desired information, negotiating, through an intermediary, a comprehension function for obscuring at least a portion of the information communicated between the first party and the second party, communicating the encrypted information to the second party, and decrypting the encrypted information using the negotiated comprehension function. Preferably, the intermediary does not itself possess sufficient information to decrypt the encrypted information, thus allowing use of an "untrusted" intermediary. The comprehension function may be dynamic with respect to its response to the negotiated comprehension function, and thus permit limitations on the use of the information by the second party. For example, the decryption of the encrypted information may be time limited.

25 Claims, 10 Drawing Sheets



U.S. PATENT DOCUMENTS

4,567,600	A	1/1986	Massey
4,575,621	A	3/1986	Dreifus
4,578,531	A	3/1986	Everhart
4,590,470	A	5/1986	Koenig
4,595,950	A	6/1986	Lofberg
4,625,076	A	11/1986	Okamoto
4,633,036	A	12/1986	Hellman
4,731,841	A	3/1988	Rosen
4,734,564	A	3/1988	Boston
4,736,203	A	4/1988	Sidlauskas
4,752,676	A	6/1988	Leonard
4,812,628	A	3/1989	Boston
4,819,267	A	4/1989	Cargile
4,827,518	A	5/1989	Feustel
4,868,376	A	9/1989	Lessin et al.
4,890,323	A	12/1989	Beker
4,896,363	A	1/1990	Taylor
4,926,325	A	5/1990	Benton
4,926,480	A	5/1990	Chaum
4,941,173	A	7/1990	Boule
4,952,928	A	8/1990	Carroll
4,961,142	A	10/1990	Elliott
4,972,476	A	11/1990	Nathans
4,977,595	A	12/1990	Ohta
4,993,068	A	2/1991	Piosenka
5,020,105	A	5/1991	Rosen
5,036,461	A	7/1991	Elliott
5,056,141	A	10/1991	Dyke
5,056,147	A	10/1991	Turner
5,478,993	A	12/1995	Derksen
5,481,613	A	1/1996	Ford
5,483,601	A	1/1996	Faulkner
5,485,312	A	1/1996	Horner
5,485,519	A	1/1996	Weiss
5,497,430	A	3/1996	Sadovnik
5,499,293	A	3/1996	Behram
5,508,912	A	4/1996	Schneiderman
5,511,121	A	4/1996	Yacobi
5,519,778	A	5/1996	Leighton
5,521,722	A	5/1996	Colvill
5,523,739	A	6/1996	Manneschi
5,526,428	A	6/1996	Arnold
5,528,492	A	6/1996	Fukushima
5,528,516	A	6/1996	Yemini
5,533,123	A	7/1996	Force
5,534,855	A	7/1996	Shockley
5,535,383	A	7/1996	Gower
5,544,255	A	8/1996	Smithies
5,546,462	A	8/1996	Indeck
5,546,580	A	8/1996	Seliger
5,553,145	A	9/1996	Micali
5,553,155	A	9/1996	Kuhns
5,557,765	A	9/1996	Lipner
5,559,885	A	9/1996	Drexler
5,561,718	A	10/1996	Trew
5,572,596	A	11/1996	Wildes
5,578,808	A	11/1996	Taylor
5,579,393	A	11/1996	Conner
5,583,933	A	12/1996	Mark
5,583,950	A	12/1996	Prokoski
5,586,171	A	12/1996	McAllister
5,586,262	A	12/1996	Komatsu
5,588,059	A	12/1996	Chandes
5,592,408	A	1/1997	Keskin
5,592,549	A	1/1997	Nagel
5,592,945	A	1/1997	Fiedler
5,594,806	A	1/1997	Colbert
5,604,804	A	2/1997	Micali
5,606,609	A	2/1997	Houser
5,608,387	A	3/1997	Davies
5,613,004	A	3/1997	Cooperman
5,613,012	A	3/1997	Hoffman
5,615,277	A	3/1997	Hoffman
5,616,904	A	4/1997	Fernadez
5,619,991	A	4/1997	Sloane
5,621,201	A	4/1997	Langhans
5,621,889	A	4/1997	Lermuzeaux
5,623,547	A	4/1997	Jones
5,623,601	A	4/1997	Vu
5,629,980	A	5/1997	Stefik
5,629,982	A	5/1997	Micali
5,631,961	A	5/1997	Mills
5,632,011	A	5/1997	Landfield
5,633,932	A	5/1997	Davis
5,634,012	A	5/1997	Stefik
5,636,282	A	6/1997	Holmquist
5,636,292	A	6/1997	Rhoads
5,638,443	A	6/1997	Stefik
5,644,778	A	7/1997	Burks
5,646,839	A	7/1997	Katz
5,646,997	A	7/1997	Barton
5,647,017	A	7/1997	Smithies
5,647,364	A	7/1997	Schneider
5,659,616	A	8/1997	Sudia
5,659,726	A	8/1997	Sandford
5,664,018	A	9/1997	Leighton
5,664,109	A	9/1997	Johnson
5,666,400	A	9/1997	McAllister
5,666,414	A	9/1997	Micali
5,666,416	A	9/1997	Micali
5,666,420	A	9/1997	Micali
5,668,878	A	9/1997	Brands
5,677,955	A	10/1997	Doggett
5,679,940	A	10/1997	Templeton
5,680,460	A	10/1997	Tomko
5,682,032	A	10/1997	Philipp
5,682,142	A	10/1997	Loosmore
5,687,236	A	11/1997	Moskowitz
5,696,827	A	12/1997	Brands
5,696,908	A	12/1997	Muehlberger
5,699,427	A	12/1997	Chow
5,703,562	A	12/1997	Nilsen
5,706,427	A	1/1998	Tabuki
5,710,834	A	1/1998	Rhoads
5,712,912	A	1/1998	Tomko
5,712,914	A	1/1998	Aucsmith
5,715,403	A	2/1998	Stefik
5,717,757	A	2/1998	Micali
5,719,950	A	2/1998	Osten
5,727,092	A	3/1998	Sandford
5,734,154	A	3/1998	Jachimowicz
5,734,752	A	3/1998	Knox
5,737,419	A	4/1998	Ganesan
5,737,420	A	4/1998	Tomko
5,740,244	A	4/1998	Indeck
5,742,683	A	4/1998	Lee
5,742,685	A	4/1998	Berson
5,745,555	A	4/1998	Mark
5,745,569	A	4/1998	Moskowitz
5,745,573	A	4/1998	Lipner
5,745,604	A	4/1998	Rhoads
5,748,738	A	5/1998	Bisbee
5,748,763	A	5/1998	Rhoads
5,748,783	A	5/1998	Rhoads
5,748,890	A	5/1998	Goldberg
5,751,809	A	5/1998	Davis
5,751,836	A	5/1998	Wildes
5,751,909	A	5/1998	Gower
5,754,939	A	5/1998	Herz
5,757,431	A	5/1998	Bradley
5,757,916	A	5/1998	MacDoran
5,761,288	A	6/1998	Pinard
5,761,298	A	6/1998	Davis
5,761,686	A	6/1998	Bloomberg

5,763,862	A		6/1998	Jachimowicz
5,764,789	A		6/1998	Pare
5,765,152	A		6/1998	Erickson
5,767,496	A		6/1998	Swartz
5,768,382	A		6/1998	Schneier
5,768,385	A		6/1998	Simon
5,768,388	A		6/1998	Goldwasser
5,768,426	A		6/1998	Rhoads
5,770,849	A		6/1998	Novis
5,771,071	A		6/1998	Bradley
5,772,585	A		6/1998	Lavin
5,774,551	A		6/1998	Wu
5,778,102	A		7/1998	Sandford
5,778,882	A		7/1998	Raymond
5,779,634	A		7/1998	Ema
5,781,890	A		7/1998	Nematbakhsh
5,784,461	A		7/1998	Shaffer
5,784,463	A		7/1998	Chen
5,784,566	A		7/1998	Viavant
5,787,187	A		7/1998	Bouchard
5,789,733	A		8/1998	Jachimowicz
5,790,665	A		8/1998	Micali
5,790,668	A		8/1998	Tomko
5,790,674	A		8/1998	Houvener
5,790,703	A		8/1998	Wang
5,793,868	A		8/1998	Micali
5,796,841	A		8/1998	Cordery
5,797,128	A		8/1998	Birnbaum
5,799,083	A		8/1998	Brothers
5,799,086	A		8/1998	Sudia
5,799,087	A		8/1998	Rosen
5,799,088	A		8/1998	Raike
5,802,199	A		9/1998	Pare
5,805,719	A		9/1998	Pare
5,805,803	A		9/1998	Birrell
5,812,398	A		9/1998	Nielsen
5,812,668	A		9/1998	Weber
5,812,670	A		9/1998	Micali
5,815,252	A		9/1998	Price-Francis
5,815,577	A		9/1998	Clark
5,815,657	A		9/1998	Williams
5,819,289	A		10/1998	Sanford
5,822,432	A		10/1998	Moskowitz
5,822,436	A		10/1998	Rhoads
5,825,871	A		10/1998	Mark
5,825,880	A		10/1998	Sudia
5,826,014	A		10/1998	Coley
5,826,029	A		10/1998	Gore
5,828,751	A		10/1998	Walker
5,828,840	A		10/1998	Cowan
5,832,089	A		11/1998	Kravitz
5,832,119	A		11/1998	Rhoads
5,832,450	A		11/1998	Myers
5,832,464	A		11/1998	Houvener
5,832,488	A		11/1998	Eberhardt
5,835,726	A		11/1998	Shwed
5,838,792	A	*	11/1998	Ganesan 380/282
5,838,812	A		11/1998	Pare
5,839,119	A		11/1998	Krsul
5,841,122	A		11/1998	Kirchhoff
5,841,865	A		11/1998	Sudia
5,841,886	A		11/1998	Rhoads
5,841,907	A		11/1998	Javidi
5,841,978	A		11/1998	Rhoads
5,844,244	A		12/1998	Graf
5,845,253	A		12/1998	Rensimer
5,845,267	A		12/1998	Ronen
5,848,155	A		12/1998	Cox
5,848,231	A		12/1998	Teitelbaum
5,850,442	A		12/1998	Muftic
5,850,446	A		12/1998	Berger
5,850,451	A		12/1998	Sudia
5,850,481	A		12/1998	Rhoads
5,857,022	A		1/1999	Sudia
5,857,023	A		1/1999	Demers
5,862,223	A		1/1999	Walker
5,862,246	A		1/1999	Colbert
5,862,260	A		1/1999	Rhoads
5,867,578	A		2/1999	Brickell
5,867,795	A		2/1999	Novis
5,867,802	A		2/1999	Borza
5,867,821	A		2/1999	Ballantyne
5,869,822	A		2/1999	Meadows
5,870,723	A		2/1999	Pare
5,870,744	A		2/1999	Sprague
5,872,834	A		2/1999	Teitelbaum
5,872,848	A		2/1999	Romney
5,872,849	A		2/1999	Sudia
5,875,108	A		2/1999	Hoffberg
5,876,926	A		3/1999	Beecham
5,878,137	A		3/1999	Ippolito
5,878,144	A		3/1999	Aucsmith
5,881,225	A		3/1999	Worth
5,881,226	A		3/1999	Veneklase
5,884,277	A		3/1999	Khosla
5,889,474	A		3/1999	LaDue
5,889,862	A		3/1999	Ohta
5,889,863	A		3/1999	Weber
5,889,868	A		3/1999	Moskowitz
5,890,129	A		3/1999	Spurgeon
5,890,152	A		3/1999	Rapaport
5,892,824	A		4/1999	Bentson
5,892,838	A		4/1999	Brady
5,892,900	A		4/1999	Ginter
5,892,902	A		4/1999	Clark
5,897,616	A		4/1999	Kanevsky
5,898,154	A		4/1999	Rosen
5,898,830	A		4/1999	Wesinger
5,899,998	A		5/1999	McGauley
5,901,229	A		5/1999	Fujisaki
5,901,246	A		5/1999	Hoffberg
5,903,651	A		5/1999	Kocher
5,903,880	A		5/1999	Biffar
5,903,889	A		5/1999	de la Huerga
5,905,505	A		5/1999	Lesk
5,905,800	A		5/1999	Moskowitz
5,907,149	A		5/1999	Marckini
5,909,493	A		6/1999	Motoyama
5,910,988	A		6/1999	Ballard
5,911,132	A		6/1999	Sloane
5,911,143	A		6/1999	Deinhart
5,911,687	A		6/1999	Sato
5,912,818	A		6/1999	McGrady
5,912,974	A		6/1999	Holloway
5,913,025	A		6/1999	Higley
5,913,196	A		6/1999	Talmor
5,915,008	A		6/1999	Dulman
5,915,018	A		6/1999	Aucsmith
5,915,027	A		6/1999	Cox
5,915,087	A		6/1999	Hammond
5,915,093	A		6/1999	Berlin
5,915,240	A		6/1999	Karpf
5,915,973	A		6/1999	Hoehn-Saric
5,918,227	A		6/1999	Polnerow
5,920,058	A		7/1999	Weber
5,920,384	A		7/1999	Borza
5,920,477	A		7/1999	Hoffberg
5,920,628	A		7/1999	Indeck
5,920,629	A		7/1999	Rosen
5,920,630	A		7/1999	Wertheimer
5,923,763	A		7/1999	Walker
5,924,074	A		7/1999	Evans
5,925,126	A		7/1999	Hsieh
5,926,548	A		7/1999	Okamoto
5,928,333	A		7/1999	Landfield
5,930,369	A		7/1999	Cox

5,930,759	A		7/1999	Moore
5,930,777	A		7/1999	Barber
5,933,498	A		8/1999	Schneck
5,933,515	A		8/1999	Pu
5,933,809	A		8/1999	Hunt
5,935,071	A		8/1999	Schneider
5,937,068	A		8/1999	Audebert
5,937,394	A		8/1999	Wong
5,940,508	A	*	8/1999	Long et al. 380/273
5,943,422	A		8/1999	Van Wie
5,943,423	A		8/1999	Muftic
5,943,424	A		8/1999	Berger
5,944,823	A		8/1999	Jade
5,946,414	A		8/1999	Cass
5,946,669	A		8/1999	Polk
5,948,136	A		9/1999	Smyers
5,949,045	A		9/1999	Ezawa
5,949,046	A		9/1999	Kenneth
5,949,866	A		9/1999	Coiera
5,949,876	A		9/1999	Ginter
5,949,877	A		9/1999	Traw
5,949,879	A		9/1999	Berson
5,949,881	A		9/1999	Davis
5,949,882	A		9/1999	Angelo
5,949,885	A		9/1999	Leighton
5,950,195	A		9/1999	Stockwell
5,951,055	A		9/1999	Mowry
5,952,638	A		9/1999	Demers
5,952,641	A		9/1999	Korshun
5,953,419	A		9/1999	Lohstroh
5,954,583	A		9/1999	Green
5,956,400	A		9/1999	Chaum
5,956,408	A		9/1999	Arnold
5,958,016	A		9/1999	Chang
5,958,050	A		9/1999	Griffin
5,960,083	A		9/1999	Micali
5,960,177	A		9/1999	Tanno
5,963,648	A		10/1999	Rosen
5,963,657	A		10/1999	Bowker
5,963,908	A		10/1999	Chadha
5,963,924	A		10/1999	Williams
5,966,446	A		10/1999	Davis
5,966,448	A	*	10/1999	Namba et al. 380/33
5,968,176	A		10/1999	Nessett
5,970,143	A		10/1999	Schneier
5,974,146	A		10/1999	Randle
5,974,389	A		10/1999	Clark
5,974,548	A		10/1999	Adams
5,978,475	A		11/1999	Schneier
5,978,494	A		11/1999	Zhang
5,978,840	A		11/1999	Nguyen
5,978,918	A		11/1999	Scholnick
5,979,773	A		11/1999	Findley
5,982,520	A		11/1999	Weiser
5,982,891	A		11/1999	Ginter
5,982,894	A		11/1999	McCalley
5,983,208	A		11/1999	Haller
5,983,350	A		11/1999	Minear
5,984,366	A		11/1999	Priddy
5,986,746	A		11/1999	Metz
5,987,132	A		11/1999	Rowney
5,987,140	A		11/1999	Rowney
5,987,153	A		11/1999	Chan
5,987,155	A		11/1999	Dunn
5,987,440	A		11/1999	O'Neil
5,987,459	A		11/1999	Swanson
5,991,399	A		11/1999	Graunke
5,991,406	A		11/1999	Lipner
5,991,408	A		11/1999	Pearson
5,991,429	A		11/1999	Coffin
5,991,431	A		11/1999	Borza
5,991,519	A		11/1999	Benhammou
5,991,731	A		11/1999	Colon
5,991,758	A		11/1999	Ellard
5,991,877	A		11/1999	Luckenbaugh
5,991,878	A		11/1999	McDonough
5,995,625	A		11/1999	Sudia
5,995,630	A		11/1999	Borza
5,995,943	A		11/1999	Bull
5,996,076	A		11/1999	Rowney
5,999,095	A		12/1999	Earl
5,999,629	A	*	12/1999	Heer et al. 705/51
5,999,637	A		12/1999	Toyoda
5,999,919	A		12/1999	Jarecki
5,999,973	A		12/1999	Glitho
6,002,756	A		12/1999	Lo
6,002,767	A		12/1999	Kramer
6,002,770	A		12/1999	Tomko
6,002,772	A		12/1999	Saito
6,003,084	A		12/1999	Green
6,003,135	A		12/1999	Bialick
6,003,765	A		12/1999	Okamoto
6,004,276	A		12/1999	Wright
6,005,859	A		12/1999	Harvell
6,005,939	A		12/1999	Fortenberry
6,005,943	A		12/1999	Cohen
6,006,328	A		12/1999	Drake
6,006,332	A		12/1999	Rabne
6,009,177	A		12/1999	Sudia
6,009,430	A		12/1999	Joseph
6,009,475	A		12/1999	Shrader
6,009,526	A		12/1999	Choi
6,011,858	A		1/2000	Stock
6,012,035	A		1/2000	Freeman
6,012,039	A		1/2000	Hoffman
6,012,049	A		1/2000	Kawan
6,012,088	A		1/2000	Li
6,014,666	A		1/2000	Helland
6,016,318	A		1/2000	Tomoike
6,016,476	A		1/2000	Maes
6,016,484	A		1/2000	Williams
6,018,724	A		1/2000	Arent
6,018,739	A		1/2000	McCoy
6,018,801	A		1/2000	Palage
6,021,202	A		2/2000	Anderson
6,021,393	A		2/2000	Honda
6,021,399	A		2/2000	Demers
6,021,491	A		2/2000	Renaud
6,021,497	A		2/2000	Bouthillier
6,023,762	A		2/2000	Dean
6,023,765	A		2/2000	Kuhn
6,026,163	A		2/2000	Micali
6,026,166	A		2/2000	LeBourgeois
6,026,167	A		2/2000	Aziz
6,026,193	A		2/2000	Rhoads
6,026,379	A		2/2000	Haller
6,026,490	A		2/2000	Johns-Vano
6,028,932	A		2/2000	Park
6,028,933	A		2/2000	Heer
6,028,936	A		2/2000	Hillis
6,028,937	A		2/2000	Tatebayashi
6,028,939	A		2/2000	Yin
6,029,067	A		2/2000	Pfundstein
6,029,150	A		2/2000	Kravitz
6,029,151	A		2/2000	Nikander
6,029,160	A		2/2000	Cabrera
6,029,195	A		2/2000	Herz
6,029,245	A		2/2000	Scanlan
6,029,247	A		2/2000	Ferguson
6,031,910	A		2/2000	Deindl
6,031,913	A		2/2000	Hassan
6,031,914	A		2/2000	Tewfik
6,032,118	A		2/2000	Jello
6,034,605	A		3/2000	March
6,034,618	A		3/2000	Tatebayashi
6,035,041	A		3/2000	Frankel

6,035,276	A	3/2000	Newman
6,035,398	A	3/2000	Bjorn
6,035,402	A	3/2000	Vaeth
6,035,406	A	3/2000	Moussa
6,037,870	A	3/2000	Alessandro
6,038,315	A	3/2000	Strait
6,038,316	A	3/2000	Dwork
6,038,322	A	3/2000	Harkins
6,038,337	A	3/2000	Lawrence
6,038,560	A	3/2000	Wical
6,038,563	A	3/2000	Bapat
6,038,581	A	3/2000	Aoki
6,038,665	A	3/2000	Bolt
6,038,666	A	3/2000	Hsu
6,040,783	A	3/2000	Houvener
6,041,122	A	3/2000	Graunke
6,041,123	A	3/2000	Colvin
6,041,349	A	3/2000	Sugauchi
6,041,355	A	3/2000	Toga
6,041,357	A	3/2000	Kunzelman
6,041,408	A	3/2000	Nishioka
6,041,410	A	3/2000	Hsu
6,041,411	A	3/2000	Wyatt
6,041,412	A	3/2000	Timson
6,042,005	A	3/2000	Basile
6,044,131	A	3/2000	McEvoy
6,044,155	A	3/2000	Thomlinson
6,044,157	A	3/2000	Uesaka
6,044,205	A	3/2000	Reed
6,044,349	A	3/2000	Tolopka
6,044,350	A	3/2000	Weiant
6,044,388	A	3/2000	DeBellis
6,044,401	A	3/2000	Harvey
6,044,462	A	3/2000	Zubeldia
6,044,463	A	3/2000	Kanda
6,044,464	A	3/2000	Shamir
6,044,466	A	3/2000	Anand
6,044,468	A	3/2000	Osmond
6,045,039	A	4/2000	Stinson
6,047,051	A	4/2000	Ginzboorg
6,047,066	A	4/2000	Brown
6,047,067	A	4/2000	Rosen
6,047,072	A	4/2000	Field
6,047,242	A	4/2000	Benson
6,047,268	A	4/2000	Bartoli
6,047,269	A	4/2000	Biffar
6,047,322	A	4/2000	Vaid
6,047,325	A	4/2000	Jain
6,047,374	A	4/2000	Barton
6,047,887	A	4/2000	Rosen
6,049,610	A	4/2000	Crandall
6,049,612	A	4/2000	Fielder
6,049,613	A	4/2000	Jakobsson
6,049,627	A	4/2000	Becker
6,049,671	A	4/2000	Slivka
6,049,785	A	4/2000	Gifford
6,049,786	A	4/2000	Smorodinsky
6,049,787	A	4/2000	Takahashi
6,049,838	A	4/2000	Miller
6,049,872	A	4/2000	Reiter
6,049,874	A	4/2000	McClain
6,049,875	A	4/2000	Suzuki
6,052,466	A	4/2000	Wright
6,052,467	A	4/2000	Brands
6,052,468	A	4/2000	Hillhouse
6,052,469	A	4/2000	Johnson
6,052,688	A	4/2000	Thorsen
6,052,780	A	4/2000	Glover
6,052,788	A	4/2000	Wesinger
6,055,314	A	4/2000	Spies
6,055,321	A	4/2000	Numao
6,055,494	A	4/2000	Friedman
6,055,506	A	4/2000	Frasca
6,055,508	A	4/2000	Naor
6,055,512	A	4/2000	Dean
6,055,536	A	4/2000	Shimakawa
6,055,575	A	4/2000	Paulsen
6,055,637	A	4/2000	Hudson
6,055,639	A	4/2000	Schanze
6,056,197	A	5/2000	Hara
6,056,199	A	5/2000	Wiklof
6,057,872	A	5/2000	Candalore
6,058,187	A	5/2000	Chen
6,058,188	A	5/2000	Chandersekara
6,058,189	A	5/2000	McGough
6,058,193	A	5/2000	Cordery
6,058,303	A	5/2000	Astrom
6,058,381	A	5/2000	Nelson
6,058,383	A	5/2000	Narasimhalu
6,061,448	A	5/2000	Smith
6,061,451	A	5/2000	Muratani
6,061,454	A	5/2000	malik
6,061,665	A	5/2000	Bahreman
6,061,692	A	5/2000	Thomas
6,061,729	A	5/2000	Nightingale
6,061,789	A	5/2000	Hauser
6,061,790	A	5/2000	Bodnar
6,061,791	A	5/2000	Moreau
6,061,792	A	5/2000	Simon
6,061,794	A	5/2000	Angelo
6,061,796	A	5/2000	Chen
6,061,797	A	5/2000	Jade
6,061,798	A	5/2000	Coley
6,061,799	A	5/2000	Eldridge
6,064,723	A	5/2000	Cohn
6,064,737	A	5/2000	Rhoads
6,064,738	A	5/2000	Fridrich
6,064,740	A	5/2000	Curiger
6,064,741	A	5/2000	Horn
6,064,751	A	5/2000	Smithies
6,064,764	A	5/2000	Bhaskaran
6,064,878	A	5/2000	Denker
6,064,968	A	5/2000	Schanz
6,064,977	A	5/2000	Haverstock
6,065,008	A	5/2000	Simon
6,065,119	A	5/2000	Sandford
6,065,675	A	5/2000	Teicher
6,067,466	A	5/2000	Selker
6,067,620	A	5/2000	Holden
6,068,184	A	5/2000	Barnett
6,069,647	A	5/2000	Sullivan
6,069,914	A	5/2000	Cox
6,069,952	A	5/2000	Saito
6,069,954	A	5/2000	Moreau
6,069,955	A	5/2000	Coppersmith
6,069,969	A	5/2000	Keagy
6,069,970	A	5/2000	Salatino
6,070,141	A	5/2000	Houvener
6,070,239	A	5/2000	McManis
6,072,870	A	6/2000	Nguyen
6,072,874	A	6/2000	Shin
6,072,876	A	6/2000	Obata
6,072,894	A	6/2000	Payne
6,073,106	A	6/2000	Rozen
6,073,125	A	6/2000	Cordery
6,073,160	A	6/2000	Grantham
6,073,172	A	6/2000	Frailong
6,073,234	A	6/2000	Kigo
6,073,236	A	6/2000	Kusakabe
6,073,237	A	6/2000	Ellison
6,073,238	A	6/2000	Drupsteen
6,073,240	A	6/2000	Kurtzberg
6,073,242	A	6/2000	Hardy
6,075,455	A	6/2000	DiMaria
6,075,852	A	6/2000	Ashworth
6,075,854	A	6/2000	Copley

6,075,860 A 6/2000 Ketcham
6,075,861 A 6/2000 Miller
6,075,864 A 6/2000 Batten
6,075,865 A 6/2000 Scheidt
6,076,066 A 6/2000 DiRienzo
6,076,077 A 6/2000 Saito
6,076,078 A 6/2000 Camp
6,076,162 A 6/2000 Deindl
6,076,163 A 6/2000 Hoffstein
6,076,164 A 6/2000 Tanaka
6,076,166 A 6/2000 Moshfeghi
6,076,167 A 6/2000 Borza
6,078,265 A 6/2000 Bonder
6,078,586 A 6/2000 Dugan
6,078,663 A 6/2000 Yamamoto
6,078,665 A 6/2000 Anderson
6,078,667 A 6/2000 Johnson
6,078,909 A 6/2000 Knutson
6,078,946 A 6/2000 Johnson
6,079,018 A 6/2000 Hardy
6,079,020 A 6/2000 Liu
6,079,021 A 6/2000 Abadi
6,079,047 A 6/2000 Cotugno
6,079,621 A 6/2000 Vardanyan
6,081,199 A 6/2000 Hogl
6,081,533 A 6/2000 Laubach
6,081,597 A 6/2000 Hoffstein
6,081,598 A 6/2000 Dai
6,081,610 A 6/2000 Dwork
6,081,750 A 6/2000 Hoffberg
6,081,790 A 6/2000 Rosen
6,081,793 A 6/2000 Challener
6,081,893 A 6/2000 Frawrock
6,081,900 A 6/2000 Subramanian
6,082,776 A 7/2000 Feinberg
6,092,724 A 7/2000 Bouthillier
6,108,644 A 8/2000 Goldschlag
6,108,787 A 8/2000 Anderson
6,112,181 A 8/2000 Shear
6,118,874 A 9/2000 Okamoto
6,119,229 A 9/2000 Martinez
6,125,186 A 9/2000 Saito
6,128,391 A * 10/2000 Denno et al. 380/283
6,131,090 A 10/2000 Basso
6,134,326 A 10/2000 Micali
6,134,328 A 10/2000 Cordery
6,137,884 A 10/2000 Micali
6,138,119 A 10/2000 Hall
6,141,750 A 10/2000 Micali
6,141,755 A 10/2000 Dowd
6,141,758 A 10/2000 Benantar
6,145,079 A 11/2000 Mitty
6,148,338 A 11/2000 Lachelt
6,148,342 A 11/2000 Ho
6,149,440 A 11/2000 Clark
6,151,395 A 11/2000 Harkins
6,157,721 A 12/2000 Shear
6,157,914 A 12/2000 Seto
6,158,010 A 12/2000 Moriconi
6,161,139 A 12/2000 Win
6,161,181 A 12/2000 Haynes
6,169,802 B1 * 1/2001 Lerner et al. 380/44
6,175,626 B1 1/2001 Aucsmith
6,192,472 B1 2/2001 Garay
6,192,473 B1 2/2001 Ryan
6,192,476 B1 2/2001 Gong
6,236,727 B1 5/2001 Ciacelli
6,263,436 B1 7/2001 Franklin et al.
6,363,154 B1 3/2002 Peyravian
6,393,127 B2 5/2002 Vogler
6,405,313 B1 6/2002 Reiter et al.
6,411,716 B1 6/2002 Brickell
6,438,694 B2 * 8/2002 Saito 713/189
6,446,051 B1 9/2002 Gupta
6,529,885 B1 3/2003 Johnson
6,567,850 B1 5/2003 Freishtat
6,641,050 B2 * 11/2003 Kelley et al. 235/492
6,671,759 B1 * 12/2003 Noda et al. 710/104
6,779,111 B1 * 8/2004 Gehrmann et al. 713/171
6,859,533 B1 * 2/2005 Wang et al. 380/28
6,937,726 B1 * 8/2005 Wang 380/30

OTHER PUBLICATIONS

Markus Jakobsson, "On Quorum Controlled Asymmetric Proxy Re-encryption, Public Key Cryptography", LNCS 1560. Springer-Verlag, 1999. pp. 112-121. http://citeseer.ist.psu.edu/context/574339/0.*

Tatsuaki Okamoto, "Threshold- Key-Recovery System for RSA", Security Protocols Workshop,Paris, 1997. http://citeseer.ist.psu.edu/okamoto97threshold.html.*

M. Abadi, M. Burrows, B. Lampson, G. Plotkin A Calculus for Access Control in Distributed Systems, ACM Transactions on Programming Languages and Systems, 15(4):706-734 (1993).

E. Alderman and C. Kennedy, The Right to Privacy (Alfred A. Knopf, publisher, 1995): 140-143, 323-332.

E. Barker, NIST Cryptographic Toolkit, National Information Security Conference (Oct. 16, 2000) *reprinted at* csrc.nist.gov/encryption/aes/rijndael/nissc4pdf.

J. Barkley, Role-Based Access Control for the World Wide Web, *reprinted at* http://hissa.ncsl.nist.gov/rbac.

P. Beauchemin, G. Brassard, A Generalization of Hellman's Extension of Shannon's Approach to Cryptography, Advances in Cryptology-CRYPTO '87, Lecture Notes in Computer Science No. 293, p. 461.

A. Beimel, M. Burmester, Y. Desmedt, E. Kushilevitz, Computing Functions of a Shared Secret, SIAM J. on Discrete Mathematics, 13(3): 324-345, 2000.

M. Bellare, "Practice-Oriented Provable-Security," Proceedings of the ISW 97 conference, to appear in Springer Verlag LLNCS, 1998. or Lectures on Data Security: Modern Cryptology in Theory and Practice (I. Damgard, ed.).

M. Bellaire and S. Goldwasser, Verifiable Partial Key Escrow appearing in Proceedings of the Fourth Annual Conference on Computer and Communications Security, ACM (1997).

M. Bellare and R. Rivest, Translucent cryptography—An Alternative to Key Escrow and its Implementation via Fractional Oblivious Transfer, MIT Laboratory for Computer Science Technical Memo. 683, Feb. 1996 or Journal of Cryptology (1999) 12:117-139 or citeseer.nj.nec.com/article/bellare97translucent.html.

P. Benassi, Truste: An Online Privacy Seal Program. Communications of the ACM, 42(2): 56—59 (Feb. 1999).

C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Experimental Quantum Cryptography, J. Cryptology 5: 3—28 (1992).

S. Blackburn, S. Blake-Wilson, M. Burmester, and S. Galbraith, Shared Generation of Shared RSA Keys, Technical Report CORR98-19, Department of Combinatorics & Optimization, University of Waterloo, 1998.

D. Boneh, M. Franklin, Efficient Generation of Shared RSA Keys, Advances in Cryptology—CRYPTO '97 Lecture Notes in Computer Science, No. 1294, pp. 425-439.

D. Boneh, J. Horwitz, Generating a Product of Three Primes with an Unknown Factorization, Algorithmic Number Theory (J. Buhler, ed.)—Third International Symposium (ANTS-III), 1998, Lecture Notes in Computer Science, No. 1423, pp. 237-251.

S. Brands, Electronic Cash on the Internet.

S. Brands, Restrictive Blinding of Secret-Key Certificates, in Advances in Cryptology—EUROCRYPT '95 (L. Guillou & J. Quisquater, eds.), Lecture Notes in Computer Science, No. 921, pp. 231-247.

S. Brands, Untraceable Off-line Cash in Wallets with Observers, Advances in Cryptology—CRYPTO '93 (D. Stinson, ed.), Lecture Notes in Computer Science, No. 773, pp. 302-318.

S. Brands, Secret-Key Certificates.

J. Brandt, I. Damgard, P. Landrock, and T. Pedersen, Zero-Knowledge Authentication Scheme with Secret Key Exchange, Journal of Cryptology (1998) 11: 147-159 or Advances in Cryptology: Proceedings of Crypto '88, S. Goldwasser, ed., Lecture Notes in Computer Science 403, Springer-Verlag (1989), 583-588.

E. Brickell, A Fast Modular Multiplication Algorithm with Application to Two Key Cryptography, Advances in Cryptology—Proceedings of Crypto 82 (D. Chaum, R. Rivest, & A. Sherman, eds.), pp. 51-60 (1982).

S. Buckovich, H. Rippen and M. Rozen, Driving Toward Guiding Principles: A Goal for Privcacy, Confidentiality, and Security of Health Information, Journal of the American Medical Informatics Association 6:122-133 (1999).

V. Bush: As We May Think, The Atlantic Monthly, 176(1): 101-108 (1945).

D. Chaum, Achieving Electronic Privacy, Scientific American, Aug. 1992, p. 96-101.

D. Chaum, "Blind Signatures for Untraceable Payments", Advances in Cryptology—Proceedings of Crypto 82 (D. Chaum, R. Rivest, & A. Sherman, eds., 1982), pp. 199-203.

D. Chaum, The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability, Journal of Cryptology (1988) 1: 65-75.

J. Cimino, Beyond the Superhighway: Exploiting the Internet with Medical Informatics, Journal of the American Medical Informatics Association, 4: 279-284 (1997).

R. Clarke, "Internet Privacy Concerns Confirm the Case for Intervention", Communications of the ACM, 42(2): 60-67 (Feb. 1999).

M. Collen, A Vision of Health Care and Informatics in 2008, Journal of the American Medical Informatics Association 6:1-5 (1999).

Common Markup for micropayment per fee links, http://www.w3.org/TR/1999/WD-Micropayment-Markup-19990825 (Aug. 25, 1999).

Common Markup for web Micropayment Systems, http://www.3.org/TR/1999/WD-Micropayment-Markup-19990609 (Jun. 9, 1999).

Computer Science and Telecommunications Board, Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure, For the Record: Protecting Electronic Health Information (P. Clayton, ed.)(1997).

Computer Science and Telecommunications Board, National Research Council, Networking Health: Prescriptions for the Internet (2000).

R. Cramer, Introduction to Secure Computation, Lectures on Data Security: Modern Cryptology in Theory and Practice, 16-62.

R. Cramer, I. Damgard, and U. Maurer, "General Secure Multi-party Computation from any Linear Secret-Sharing Scheme", in Advances in Cryptology—EUROCRYPT 2000, Lecture Notes in Computer Science, No. 1807 (Bart Preneel, Ed.), pp. 316-334.

L. Cranor. Internet Privacy, Communications of the ACM 42(2): 29-31 (Feb. 1999).

C. Crépeau, and J. Kilian, "Achieving Oblivious Transfer Using Weakened Security Assumptions," Proceedings of the 29th Annual Foundations of Computer Science(1988), IEEE, pp. 42-52.

B. Crispo, P. Landrock, V. Matyas, WWW security and trusted third party services, Future Generation Computer Systems 16: 331-341 (2000).

R. Cushman, Serious Technology Assessment for Health Care Information Technology, Journal of the American Medical Informatics Association 4:259-65 (1997).

I. Damgard, Commitment Schemes and Zero-Knowledge Protocols, in Lectures on Data Security: Modern Cryptology in Theory and Practice, Lecture Notes on Computer Science, No. 1561 (I. Damgard, ed. 1999), pp. 63-86.

E. Dawson, A. Clark, M. Looi, Key management in a non-trusted distributed environment, Future Generation Computer Systems 16: 319-329 (2000).

D. Denning, Descriptions of Key Escrow Systems (Version of Feb. 26, 1997) *reprinted at* http://www.cs.georgetown.edu/~denning/crypto/Appendix.html.

D. Denning and D. Branstad, A Taxonomy for Key Escrow Encryption Systems, Communications of the ACM, 39(3): 34-40 (Mar. 1996) *reprinted at* www.cs.georgetown.edu/~denning/crypto/Taxonomy.html.

Department of Defense, Trusted Computer System Evaluation Criteria, DoD 5200.28-STD (Dec. 26, 1985).

R. DeWitt, A. Harton, W. Hoffmann, R. Keenan, M. Russell, Patient Information and Confidentiality in Treatise on Health Care Law, §§ 16.01—16.03 (Kaufman et al., Eds., 1998).

W. Diffie and M. Hellman, "New Directions In Cryptography," I.E.E.E. Transactions on Information Theory, vol. 22: 644-654 (Nov. 1976).

W. Diffie and M. Hellman, Privacy and Authentication: An Introduction to Cryptography, *reprinted at* http://www.cs.berkeley.edu/~gribble/osprelims/summaries/priv_auth.html.

The Drummond Group, The HealthKey Program: PKI in Healthcare.

G. Durfee and P. Nguyen, Cryptanalysis of the RSA Schemes with Short Secret Exponent from Asiacrypt '99, in Advances in Cryptology—ASIACRYPT 2000, Lecture Notes in Computer Science, No. 1976 (T. Okamoto, ed.), pp. 14-29.

C. Ellison, C. Hall, R. Milbert, and B. Schneier. Protecting secret keys with personal entropy. Future Generation Computer Systems, 16(4):311-318, 2000, *available at* http://www.counterpane.com.

Ferguson v. *City of Charleston*, 532 U.S. 67 (2001).

M. Fischer, S. Micali, and C. Rackoff, A Secure Protocol for the Oblivious Transfer, Eurocrypt 1984. Journal of Cryptology 9: 191-195 (1996).

R. Frank, Security Issues in the Virtual Corporation, Computers & Security, 15: 471-476 (1996).

Y. Frankel, P. MacKenzie, M. Yung, "Robust Efficient Distributed RSA-Key Generation", Proceedings of the Seventeenth Annual ACM Symposium on Principles of Distributed Computing (1998), p. 320.

A. Froomkin, The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution, 143 University of Pennsylvania Law Review 709-897 (1995).

A. Froomkin, It Came From Planet Clipper: The Battle Over Cryptographic Key "Escrow", 1996 The University of Chicago Legal Forum 15-75 (1996).

A. Froomkin, The Essential Role of Trusted Third Parties in Electronic Commerce, 75 Oregon Law Review 49-115 (1996).

E. Gabber, P. Gibbons, D. Kristol, Y. Matias, & A. Mayer. Consistent, Yet Anonymous, Web Access with LPWA. Communications of the ACM, 42(2): 42-47 (Feb. 1999).

O. Gandy, Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace, 1996 The University of Chicago Legal Forum 77-91 (1996).

R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Robust and Efficient Sharing of RSA Functions, in Advances in Cryptology—CRYPTO '96 (N. Koblitz, ed.), Lecture Notes in Computer Science, No. 1105, pp. 157-172 (1996).

N. Gilboa, Two Party RSA Key Generation, in Advances in Cryptology—CRYPTO '99, Lecture Notes in Computer Science, vol. 1666, Springer-Verlag, pp. 116-129 (1999).

D. Gollmann, New paradigms—old paradigms?, Future Generation Computer Systems 16: 343-349 (2000).

J. Grantham, "A probable prime test with high confidence", Journal of Number Theory, 72, pp. 32-37 (1998), *reprinted at* http://www.clark.net/pub/grantham/pseudo/.

S. Gupta, A Common Key Recovery Block Format: Promoting Interoperability Between Dissimilar Key Recovery Mechanisms, Computers & Security, 19: 41-47 (2000).

S. Gupta, S. Matyas, Public Key Infrastructure: Analysis of Existing and Needed Protocols and Object Formats for Key Recovery, Computers & Security, 19: 56-69 (2000).

J. Halamka, P. Szolovits, D. Rind, and C. Safran, "A WWW Implementation of National Recommendations for Protecting Electronic Health Information", Journal of the American Medical Informatics Association, 4: 458-464 (1997).

A. Halpert, Access Audit Trails:En Route to Security, Journal of AHIMA, 43-46 (Sep. 2000).

T. Hardy, Property and (Copyright) in Cyberspace, 1996 The University of Chicago Legal Forum 217-260 (1996).
Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 *et seq.* (Aug. 21, 1996).
Health Privacy Project, Summary of New Federal Health Privacy Regulations at reprinted at www.healthprivacy.org.
S. Hinde, 2001: A Privacy Odyssey, Computers & Security, 20: 21-27 (2001).
L. Hoffman, Balanced Key Escrow (Aug. 4, 1995) (GWU-ICTSP-04) *reprinted at* ftp://coast.cs.purdue.edu/pub/doc/cryptography/hoffman_balanced_escrow.html.
A. Jabri, The unicity distance: An upper bound on the probability of an eavesdropper successfully estimating the secret key, Information Processing Letters 60: 43-47 (1996).
V. Jones, N. Ching, & M. Winslett, Credentials for Privacy and Interoperation: . . . New Security Paradigms, '95 Workshop, LaJolla, Cal. Aug. 22-25, 1995.
A. Josang, I. Pedersen, D. Povey, PKI Seeks a Trusting Relationship, in Information Security and Privacy—Proceedings of the 5th Australasian Conference, ACISP 2000, Brisbane, Australia, Jul. 10-12, 2000 (E. Dawson and C. Boyd, eds.), pp. 191-205.
M. Joye, S. Yen, ID-based Secret-Key Cryptography, Operating Systems Review 32(4), pp. 33-39 (1998).
B. Kaliski, Emerging Standards for Public-Key Cryptography, Lectures on Data Security—Modern Cryptology in Theory and Practice, Lecture Notes on Computer Science, No. 1561 (I. Damgard, ed. 1999), pp. 87-104.
P. Keen, C. Ballance, S. Chan, and S. Schrump, Electronic Relationships: Trust by Design (2000).
I. Kohane, F.van Wingerde, J. Fackler, C. Cimino, P. Kilbridge, S. Murphy, H. Chueh, D. Rind, C. Safran, O. Barnett, and P. Szolovits, Sharing Electronic Medical Records Across Multiple Heterogeneous and Competing Institutions, Proceedings of the AMIA Fall Symposium 1996, pp. 608-612.
Y. Kun, G. Xin, L. Dayou, Security in Mobile Agent System: Problems and Approaches, Operating Systems Review, 34(1) 21-28 (2000).
E. Kushilevitz, S. Micali & R. Ostrovsky, "Reducibility and Completeness in Multi-Party Private Computations", Proceedings of the 35th Annual Symposium on Foundations of Computer Science (1994), IEEE, pp. 478-489.
G. Lawton, The Internet's Challenge to Privacy, IEEE Computer 31(6):16-18 (Jun. 1998).
T. Le, K. Nguyen, & V. Varadharajan , "How to Prove That a Committed Number is Prime", Advances in Cryptology—ASIACRYPT '99, Lecture Notes in Computer Science, No. 1716, pp. 208-218.
L. Lessig, The Path of Cyberlaw, 104 Yale Law Journal 1743-1755 (1995).
C. Lin, H. Sun, T. Hwang, Three-party Encrypted Key Exchange: Attacks and A Solution, Operating Systems Review 34(4), pp. 12-20 (2000).
Y. Lindell & B. Pinkas, Privacy Preserving Data Mining, Advances in Cryptology-CRYPTO 2000, 20th International Cryptography Conference, Santa Barbara, California, USA, Aug. 20-24, 2000 (M. Bellare, ed.), pp. 36-54.
M. Malkin, T. Wu, and D. Boneh. Experimenting with Shared Generation of RSA keys. In Proceedings of the Internet Society's 1999 Symposium on Network and Distributed System Security (SNDSS), 1999, pp. 43-56.
W. Mao, Verifiable Partial Key Escrow of Integer Factors (Nov. 16, 2000).
H. Maruyama and T. Imamura, Element-Wise XML Encryption, *reprinted at* http://trl.ibm.com/projects/xml/xss4j/docs/ewe-paper.html.
C. McDonald, "The Barriers to Electronic Medical Record Systems and How to Overcome Them", 4 Journal of the American Medical Informatics Association 213-221 (1997).
S. Micali, Fair Public-Key Cryptosystems in Advances in Cryptology—Proceedings of CRYPTO '92 (E. Brickell, ed.), Lecture Notes in Computer Science 740, pp. 113-138.
S Micali, Fair cryptosystems, MIT Technical Report, MIT/LCS/TR-579, Nov. 1993, MIT Laboratory for Computer Science (Nov. 1993).
Microsoft Corporation, Encryption and Decryption (Sep. 10, 1996) *reprinted at* http://msdn.microsoft.com/workshop/security/capi/PKCB/crypt4.asp *reprinted on* Feb. 10, 2001.
National Computer Security Center, A Guide to Understanding Discretionary Access Control in Trusted Systems (Sep. 30, 1987) NCSC-TG-003 *reprinted at* http://www.certec.or.kr/paper/authent/discretionary_access_control.txt.
S. Navathe and M. Donahoo, Towards Intelligent Integration of Heterogenous Information Sources, Proceedings of the 6th International Workshop on Database Reengineering and Interoperability, Mar. 1995.
J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti, and E. Roback, Computer Security Division, NIST, Report on the Development of the Advanced Encryption Standard (Oct. 2, 2000).
New York State, Public Health Law, Article 29-C (Health Care Agents and Proxies).
S. Ng, Comments on "On the Security of Three-Party Cryptographic Protocols" by Xu, Zhang and Zhu, Operating Systems Review 33(3): 5-13 (1999).
M. Oliva, Distributing Intellectual Property: a Model of Microtransaction Based Upon Metadata and Digital Signatures, http://oliva.modlang.denison.edu/olivia/RFC/09/.
J. Pastor, CRYPTOPOST™: A Cryptographic Application to Mail Processing, Journal of Cryptology 3(2): 137-146 (1991).
C. Pfleeger and D. Cooper, Security and Privacy: Promising Advances, IEEE Software, 27-32 (Sep./Oct. 1997).
V. Phan, Attacks on the RSA Cryptosystem and Some of Its Instances.
L. Pintsov and S. Vanstone, Postal Revenue Collection in the Digital Age, in Financial Cryptography, Proceedings of the 4th International Conference, FC 2000, Lecture Notes in Computer Science, No. 1962 (Y. Frankel, ed.), pp. 105-120.
G. Poupard and J. Stern, Generation of Shared RSA Keys by Two Parties, in Advances in Cryptology—ASIACRYPT'98, Lecture Notes in Computer Science, No. 1514 (K. Ohta & D. Pei, eds.), pp. 11-24, 1998.
J. Reagle and L. Cranor, The platform for privacy preferences, Communications of the ACM, 42(2): 48-55 (1999).
M. Reiter and A. Rubin, Anonymous Web Transactions with Crowds, Communications of the ACM, 42(2):32-38 (1999).
D. Rind, I. Kohane, P. Szolovits, C. Safran, H. Chueh, and G. Barnett, Maintaining the Confidentiality of Medical Records Shared over the Internet and the World Wide Web, Annals of Internal Medicine 127: 138-141 (1997(2)).
T. Rindfleisch, Privacy, Information Technology and Healthcare, Communications of the ACM, 40(8): 92-100 (1997).
R. Rivest and A. Shamir, "PayWord and MicroMint: Two Simple Micropayment Schemes" (May 7, 1996); Micro PAYMENT transfer Protocol (MPTP) Version 0.1 (Nov. 22, 1995) *et seq.,* http://www.w3.org/pub/WWW/TR/WD-mptp.
R. Rivest, A. Shamir, and L. Adleman: "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM 21(2): 120-126 (1978).
J. Roberts, S. Decter, and D. Nagel, Letter to the Editor [regarding Confidentiality and Electronic Medical Records], Annals of Internal Medicine 128(6): 510-511 (Mar. 15, 1998).
A. Rubin, Kerberos Versus the Leighton-Micali Protocol, Dr. Dobb's Journal, 21-26 (Nov. 2000).
C. Safran, D. Rind, M. Citroen, A. Bakker, W. Slack, and H. Bleich, Protection of Confidentiality in the Computer-Based Patient Record, MD Computing 12(3): 187-192 (May 1995).
P. Samuelson, Liability for Defective Electronic Information, Communications of the ACM, 36(1): 21-26 (Jan. 1993).
R. Sandhu, Separation of Duties In Computerized Information Systems (1991), Proceedings of the IFIP WG 11.3 Workshop on Database Security, Halifax, U.K.
E. Shortliffe, The Next Generation Internet and Health Care: A Civics Lesson for the Informatics Community, Proceedings of AMIA Fall Symposium 1998, pp. 8-14.

P. Sklavos, A. Varvitsiotis, D. Polemi, Securing Large E-Commerce Networks, in Information Security and Privacy, Proceedings of the 5th Australasian Conference, ACISP 2000, (E. Dawson and C. Boyd, eds.), pp. 123-133.

M. Smith, P. VanOorschot, M. Willett, Cryptographic Information Recovery Using Key Recovery, Computers & Security, 19: 21-27 (2000).

S. Spalding and R. Wright. Experimental Performance of Shared RSA Modulus Generation. In Proceedings of Algorithms and Experiments (ALEX98), pp. 34-43 (1998).

M. Stefik, Trusted Systems, Scientific American, 276(3): 78-81 (Mar. 1997).

P. Szolovits, A Revolution in Electronic Medical Records Systems via the World Wide Web *reprinted at* http://www.emrs.org/publications/IAHIT.html.

P. Szolovits, J. Doyle, W. Long, I. Kohane, and S. Pauker, Guardian Angel: Patient-Centered Health Information Systems, *reprinted at* http://www.ga.org/ga/manifesto/GAtr.html.

P. Tang(editorial), "An AMIA Perspective on Proposed Regulation of Privacy of Health Information", Journal of the American Medical Informatics Association 7: 205-207 (2000).

The AES Candidates, Dr. Dobb's Journal, p. 36 (Dec. 1998).

United States Congress, Office of Technology Assessment, Protecting Privacy in Computerized Medical Information, OTA-TCT-576 (Sep. 1993).

United States Department of Health and Human Services, NCVHS, Cryptography Based Patient Identifier *reprinted at* http://ncvhs.hhs.gov/app7-4.htm.

United States Department of Health and Human Services, Standards for Privacy of Individually Identifiable Health Information; Final Rule 45 CFR Parts 160 & 164 *reprinted at* http://aspe.hhs.gov/adminsimp/final/PvcTx01.htm, *also available at* 65 Federal Register 82462 *et seq.* (Dec. 28, 2000).

United States Senate Judiciary Committee, Know the Rules: Use the Tools: Privacy in the Digital Age, *reprinted at* http://judiciary.senate.gov/privacy.htm.

S. Walker, S. Lipner, C. Ellison, D. Branstad, D. Balenson, Commercial Key Escrow *reprinted at* http://www.epic.org./crypto/key_escrow/TIS_cke.html.

L Weed, Medical Records, Medical Education, and the Patient: The Problem-Oriented Medical Record as a Basic Tool, Case Western University Press (1971).

G. Wiederhold, Trends for the Information Technology Industry (1999), *reprinted at* www-db.Stanford.edu/pub/gio/1999/miti.htm.

G. Wiederhold, Value Added Middleware: Mediators (1998), *reprinted at* http://www-db.stanford.edu/pub/gio/1998/dbpd.html.

M. Willett, Features, Attributes, Characteristics, and Traits (FACTs) of Key Recovery Schemes/Products, Computers & Security, 19(1): 28-30 (2000).

P. Wing and B. O'Higgins, Using Public-Key Infrastructures for Security and Risk Management, IEEE Communications Magazine, 71-73 (Sep. 1999).

J. Wight and J. Robillard, "Adding security to portable designs", Portable Design, 16-20 (Mar. 2000).

S. Xu, G. Zhang, and H. Zhu, On the Security of Three-Party Cryptographic Protocols. Operating Systems Review, 32(3), pp. 7-20 (Jul. 1998).

Zero Knowledge Systems, Private Credentials (Nov. 2000).

S. Dawson, Trusted Interoperation of Healthcare Information (TIHI) *reprinted at* http://www-db.stanford.edu/pub/gio/TIHI/TIHI.html.

D. Liu, K. Law, and G. Wiederhold, CHAOS: An Active Security Mediation System.

G. Wiederhold, Bioinformatics: Converting Data to Knowledge *reprinted at* http://www-db.stanford.edu/pub/gio/2000/NCR2001.htm.

G. Wiederhold and M. Bilello, A Security Mediator for Health Care Information.

G. Wiederhold and M. Bilello, Protecting Inappropriate Release of Data from Realistic Databases *reprinted at* http://www-db.stanford.edu/pub/gio/TIHI/DEXAgio.html.

US 6,009,171, 12/1999, Ciacelli (withdrawn)

* cited by examiner

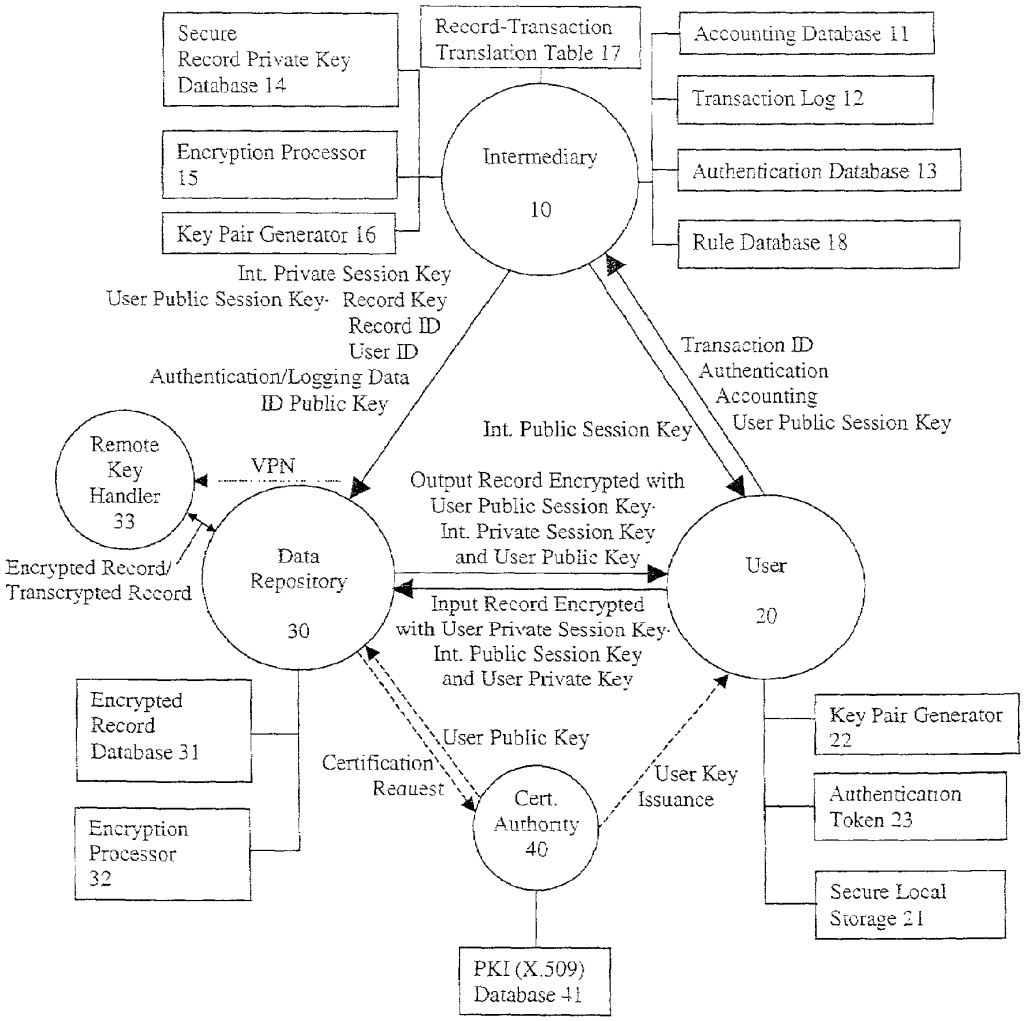

Secure
Record Private Key
Database 14
Record-Transaction
Translation Table 17
Accounting Database 11
Transaction Log 12
Encryption Processor
15
Intermediary
10
Authentication Database 13
Key Pair Generator 16
Rule Database 18
Int. Private Session Key
User Public Session Key· Record Key
Record ID
User ID
Authentication/Logging Data
ID Public Key
Transaction ID
Authentication
Accounting
User Public Session Key
Int. Public Session Key
Remote
Key
Handler
33
VPN
Output Record Encrypted with
User Public Session Key·
Int. Private Session Key
and User Public Key
Encrypted Record/
Transcrypted Record
Data
Repository
30
User
20
Input Record Encrypted
with User Private Session Key·
Int. Public Session Key
and User Private Key
Encrypted
Record
Database 31
User Public Key
Key Pair Generator
22
Certification
Request
User Key
Issuance
Cert.
Authority
40
Authentication
Token 23
Encryption
Processor
32
Secure Local
Storage 21
PKI (X.509)
Database 41

Fig. 1

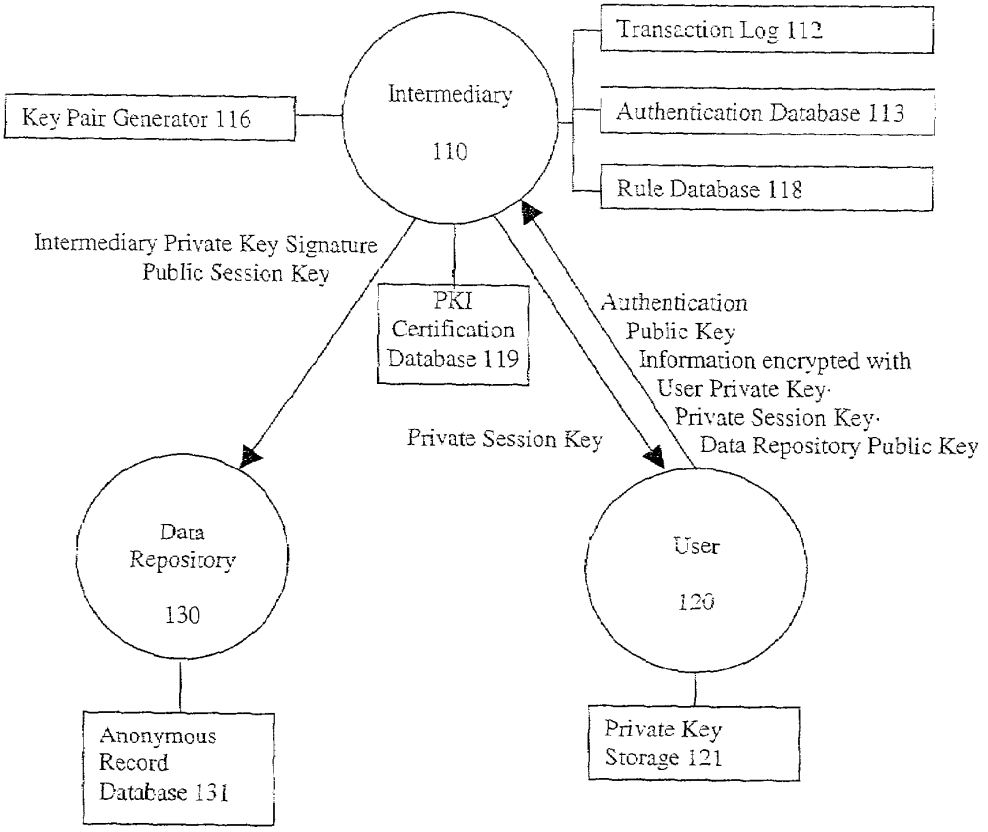

Transaction Log 112
Intermediary
110
Key Pair Generator 116
Authentication Database 113
Rule Database 118
Intermediary Private Key Signature
Public Session Key
PKI
Certification
Database 119
Authentication
Public Key
Information encrypted with
User Private Key·
Private Session Key·
Data Repository Public Key
Private Session Key
Data
Repository
130
User
120
Anonymous
Record
Database 131
Private Key
Storage 121

Fig. 2

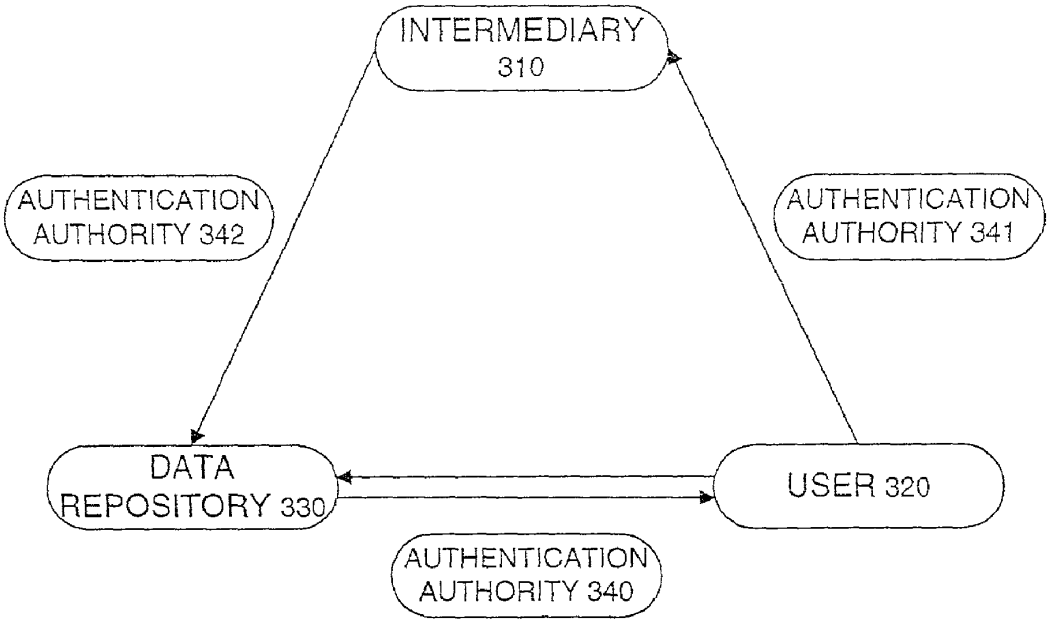

INTERMEDIARY
310
AUTHENTICATION
AUTHORITY 342
AUTHENTICATION
AUTHORITY 341
DATA
REPOSITORY 330
USER 320
AUTHENTICATION
AUTHORITY 340

Fig. 3

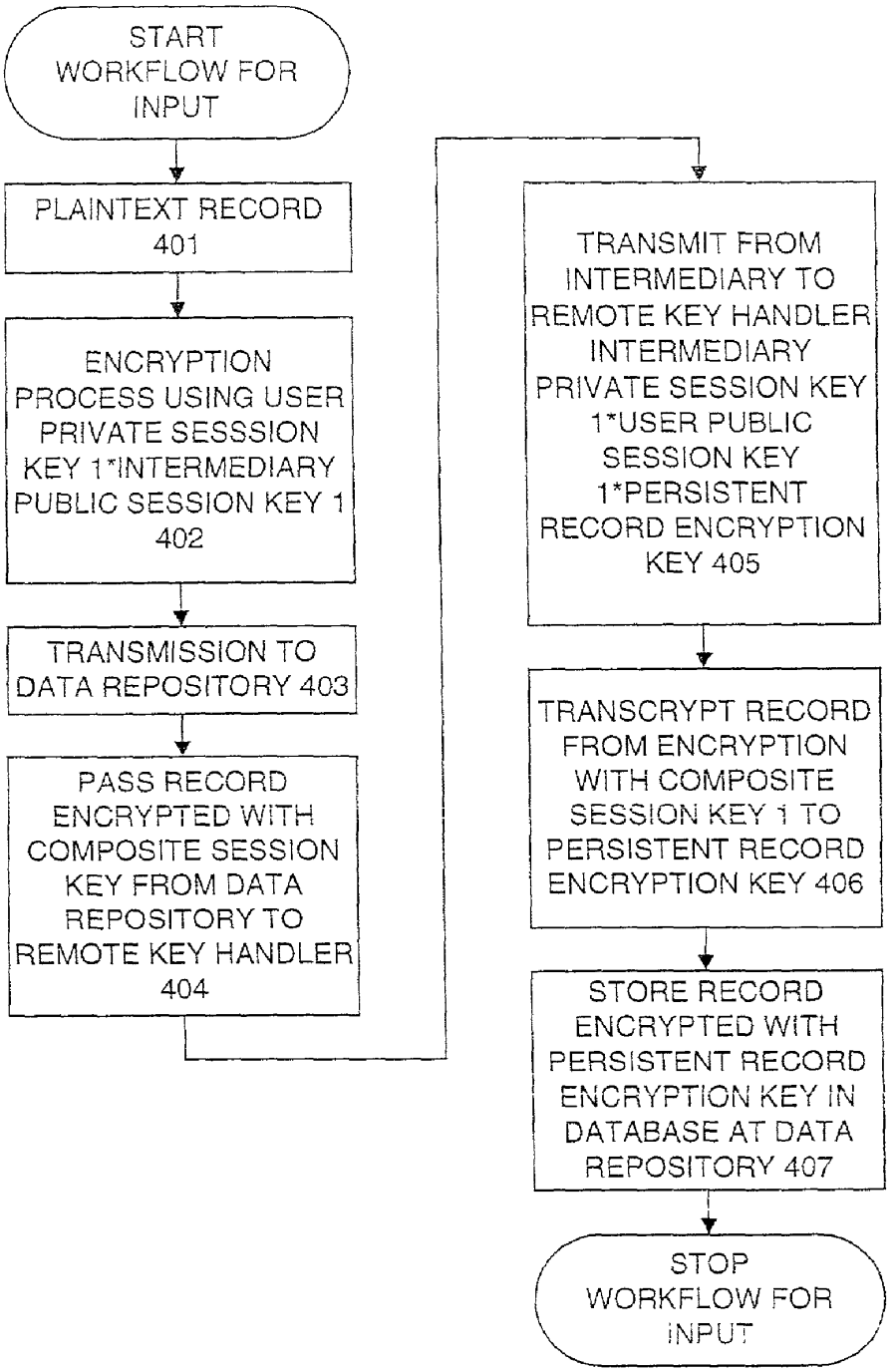

START WORKFLOW FOR INPUT
PLAINTEXT RECORD 401
ENCRYPTION PROCESS USING USER PRIVATE SESSSION KEY 1*INTERMEDIARY PUBLIC SESSION KEY 1 402
TRANSMISSION TO DATA REPOSITORY 403
PASS RECORD ENCRYPTED WITH COMPOSITE SESSION KEY FROM DATA REPOSITORY TO REMOTE KEY HANDLER 404
TRANSMIT FROM INTERMEDIARY TO REMOTE KEY HANDLER INTERMEDIARY PRIVATE SESSION KEY 1*USER PUBLIC SESSION KEY 1*PERSISTENT RECORD ENCRYPTION KEY 405
TRANSCRYPT RECORD FROM ENCRYPTION WITH COMPOSITE SESSION KEY 1 TO PERSISTENT RECORD ENCRYPTION KEY 406
STORE RECORD ENCRYPTED WITH PERSISTENT RECORD ENCRYPTION KEY IN DATABASE AT DATA REPOSITORY 407
STOP WORKFLOW FOR INPUT

Fig. 4A

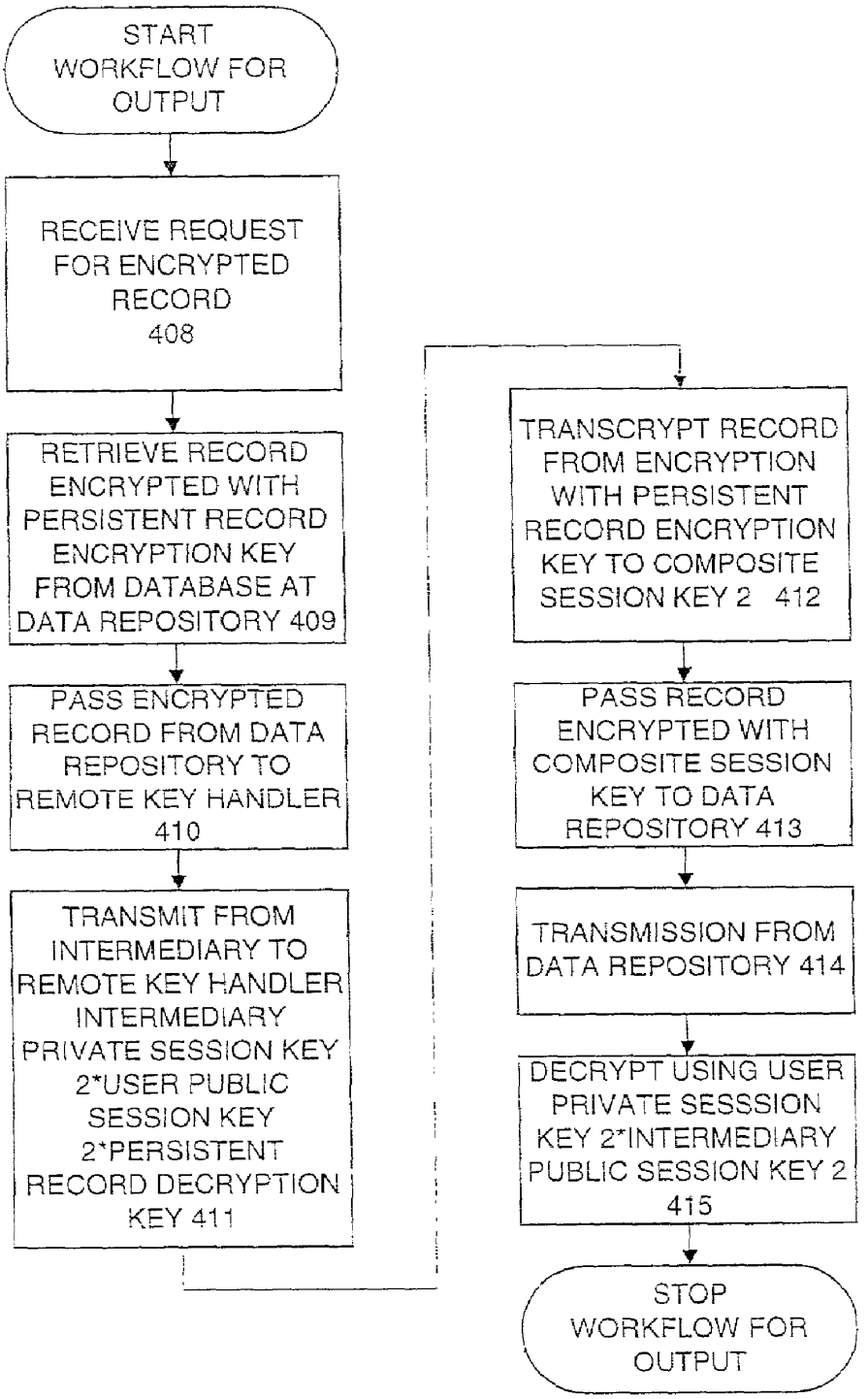

START WORKFLOW FOR OUTPUT
RECEIVE REQUEST FOR ENCRYPTED RECORD 408
RETRIEVE RECORD ENCRYPTED WITH PERSISTENT RECORD ENCRYPTION KEY FROM DATABASE AT DATA REPOSITORY 409
PASS ENCRYPTED RECORD FROM DATA REPOSITORY TO REMOTE KEY HANDLER 410
TRANSMIT FROM INTERMEDIARY TO REMOTE KEY HANDLER INTERMEDIARY PRIVATE SESSION KEY 2*USER PUBLIC SESSION KEY 2*PERSISTENT RECORD DECRYPTION KEY 411
TRANSCRYPT RECORD FROM ENCRYPTION WITH PERSISTENT RECORD ENCRYPTION KEY TO COMPOSITE SESSION KEY 2 412
PASS RECORD ENCRYPTED WITH COMPOSITE SESSION KEY TO DATA REPOSITORY 413
TRANSMISSION FROM DATA REPOSITORY 414
DECRYPT USING USER PRIVATE SESSSION KEY 2*INTERMEDIARY PUBLIC SESSION KEY 2 415
STOP WORKFLOW FOR OUTPUT

Fig. 4B

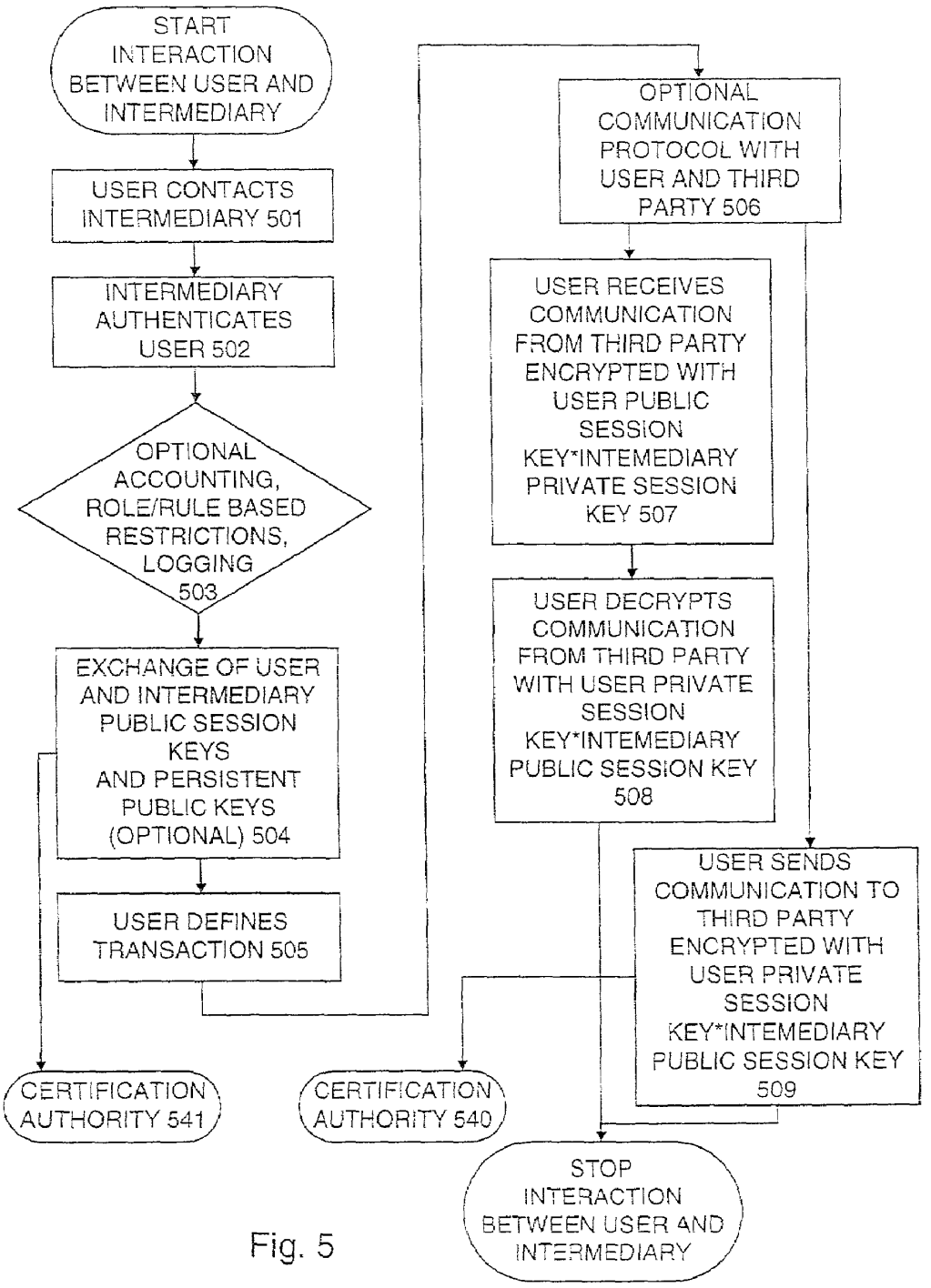

START INTERACTION BETWEEN USER AND INTERMEDIARY
USER CONTACTS INTERMEDIARY 501
INTERMEDIARY AUTHENTICATES USER 502
OPTIONAL ACCOUNTING, ROLE/RULE BASED RESTRICTIONS, LOGGING 503
EXCHANGE OF USER AND INTERMEDIARY PUBLIC SESSION KEYS AND PERSISTENT PUBLIC KEYS (OPTIONAL) 504
USER DEFINES TRANSACTION 505
OPTIONAL COMMUNICATION PROTOCOL WITH USER AND THIRD PARTY 506
USER RECEIVES COMMUNICATION FROM THIRD PARTY ENCRYPTED WITH USER PUBLIC SESSION KEY*INTEMEDIARY PRIVATE SESSION KEY 507
USER DECRYPTS COMMUNICATION FROM THIRD PARTY WITH USER PRIVATE SESSION KEY*INTEMEDIARY PUBLIC SESSION KEY 508
USER SENDS COMMUNICATION TO THIRD PARTY ENCRYPTED WITH USER PRIVATE SESSION KEY*INTEMEDIARY PUBLIC SESSION KEY 509
CERTIFICATION AUTHORITY 541
CERTIFICATION AUTHORITY 540
STOP INTERACTION BETWEEN USER AND INTERMEDIARY

Fig. 5

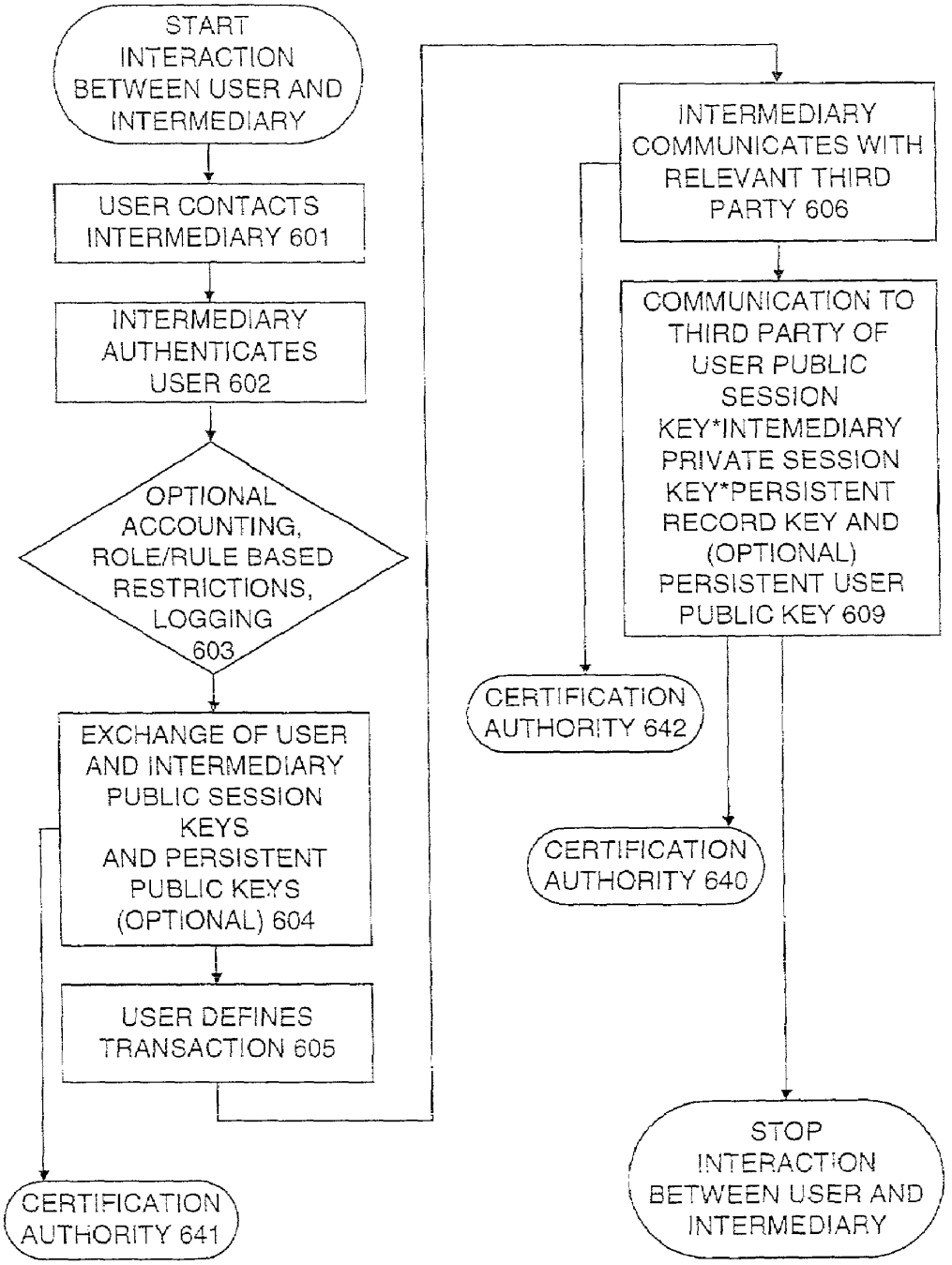

START INTERACTION BETWEEN USER AND INTERMEDIARY
USER CONTACTS INTERMEDIARY 601
INTERMEDIARY AUTHENTICATES USER 602
OPTIONAL ACCOUNTING, ROLE/RULE BASED RESTRICTIONS, LOGGING 603
EXCHANGE OF USER AND INTERMEDIARY PUBLIC SESSION KEYS AND PERSISTENT PUBLIC KEYS (OPTIONAL) 604
USER DEFINES TRANSACTION 605
CERTIFICATION AUTHORITY 641
INTERMEDIARY COMMUNICATES WITH RELEVANT THIRD PARTY 606
COMMUNICATION TO THIRD PARTY OF USER PUBLIC SESSION KEY*INTEMEDIARY PRIVATE SESSION KEY*PERSISTENT RECORD KEY AND (OPTIONAL) PERSISTENT USER PUBLIC KEY 609
CERTIFICATION AUTHORITY 642
CERTIFICATION AUTHORITY 640
STOP INTERACTION BETWEEN USER AND INTERMEDIARY

Fig. 6

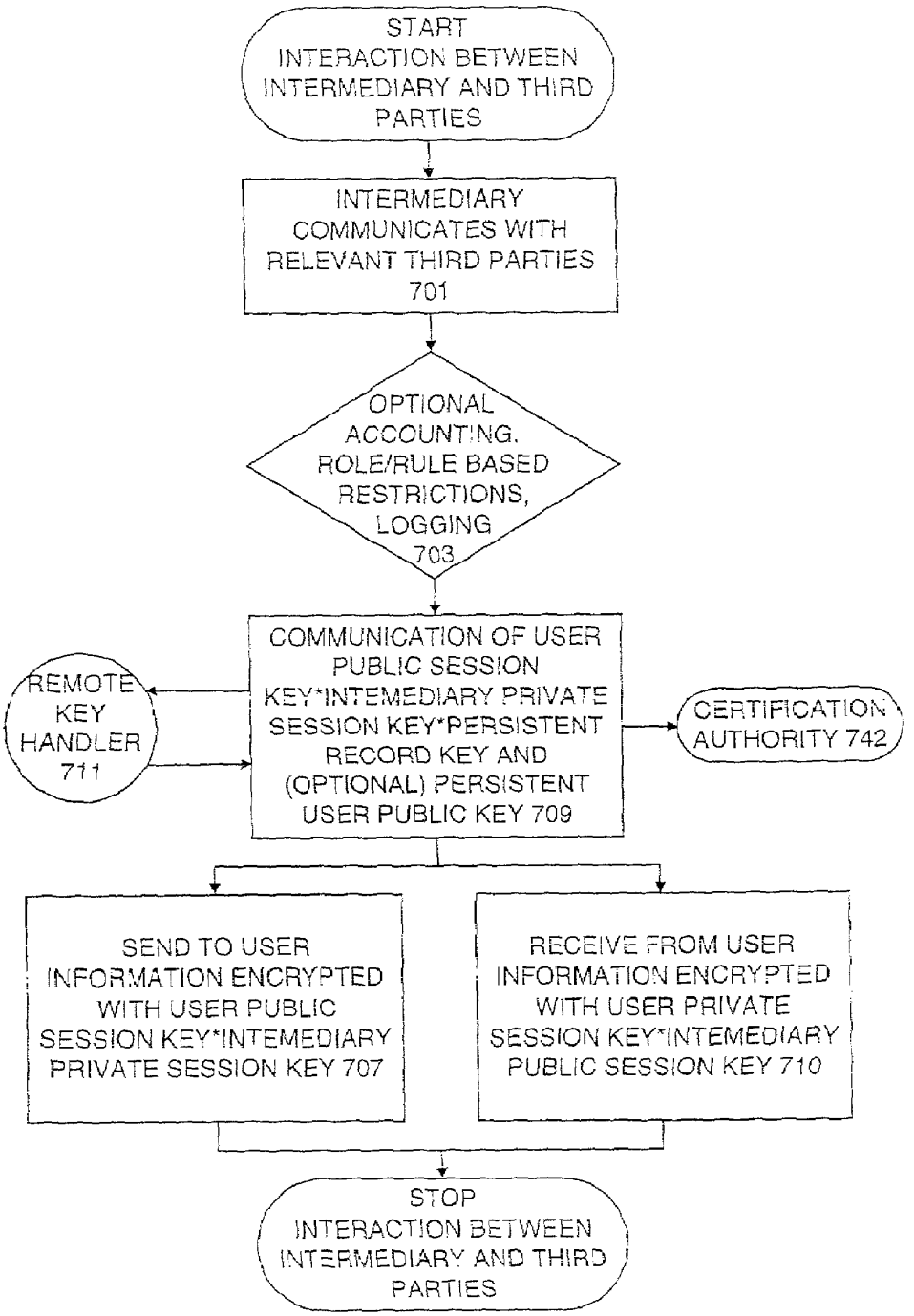

START INTERACTION BETWEEN INTERMEDIARY AND THIRD PARTIES
INTERMEDIARY COMMUNICATES WITH RELEVANT THIRD PARTIES 701
OPTIONAL ACCOUNTING, ROLE/RULE BASED RESTRICTIONS, LOGGING 703
COMMUNICATION OF USER PUBLIC SESSION KEY*INTEMEDIARY PRIVATE SESSION KEY*PERSISTENT RECORD KEY AND (OPTIONAL) PERSISTENT USER PUBLIC KEY 709
REMOTE KEY HANDLER 711
CERTIFICATION AUTHORITY 742
SEND TO USER INFORMATION ENCRYPTED WITH USER PUBLIC SESSION KEY*INTEMEDIARY PRIVATE SESSION KEY 707
RECEIVE FROM USER INFORMATION ENCRYPTED WITH USER PRIVATE SESSION KEY*INTEMEDIARY PUBLIC SESSION KEY 710
STOP INTERACTION BETWEEN INTERMEDIARY AND THIRD PARTIES

Fig. 7

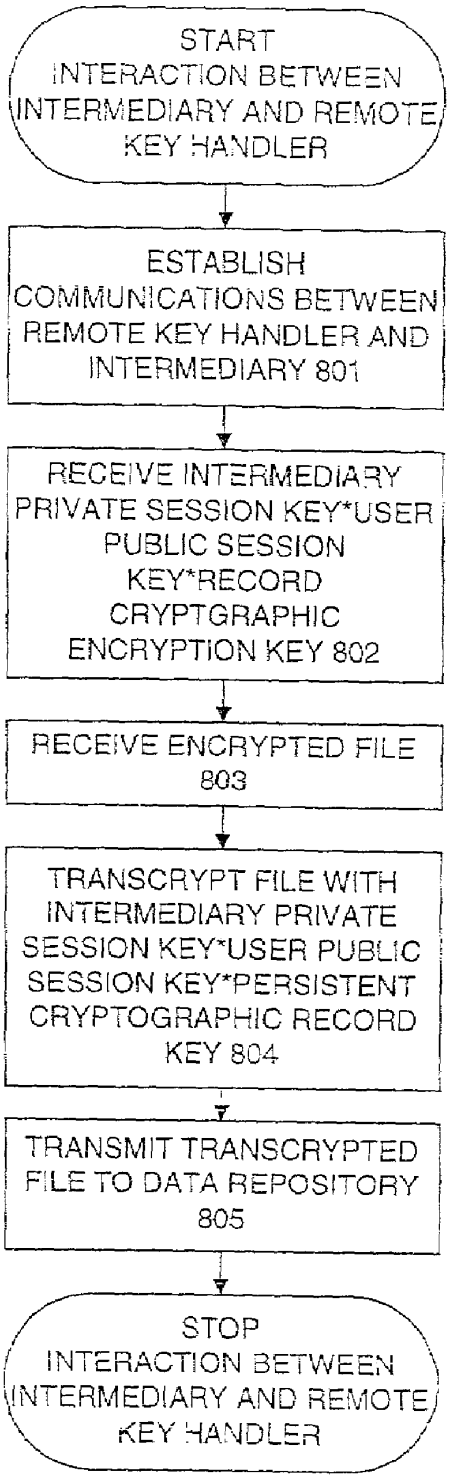

START
INTERACTION BETWEEN
INTERMEDIARY AND REMOTE
KEY HANDLER
ESTABLISH
COMMUNICATIONS BETWEEN
REMOTE KEY HANDLER AND
INTERMEDIARY 801
RECEIVE INTERMEDIARY
PRIVATE SESSION KEY*USER
PUBLIC SESSION
KEY*RECORD
CRYPTGRAPHIC
ENCRYPTION KEY 802
RECEIVE ENCRYPTED FILE
803
TRANSCRYPT FILE WITH
INTERMEDIARY PRIVATE
SESSION KEY*USER PUBLIC
SESSION KEY*PERSISTENT
CRYPTOGRAPHIC RECORD
KEY 804
TRANSMIT TRANSCRYPTED
FILE TO DATA REPOSITORY
805
STOP
INTERACTION BETWEEN
INTERMEDIARY AND REMOTE
KEY HANDLER

Fig. 8

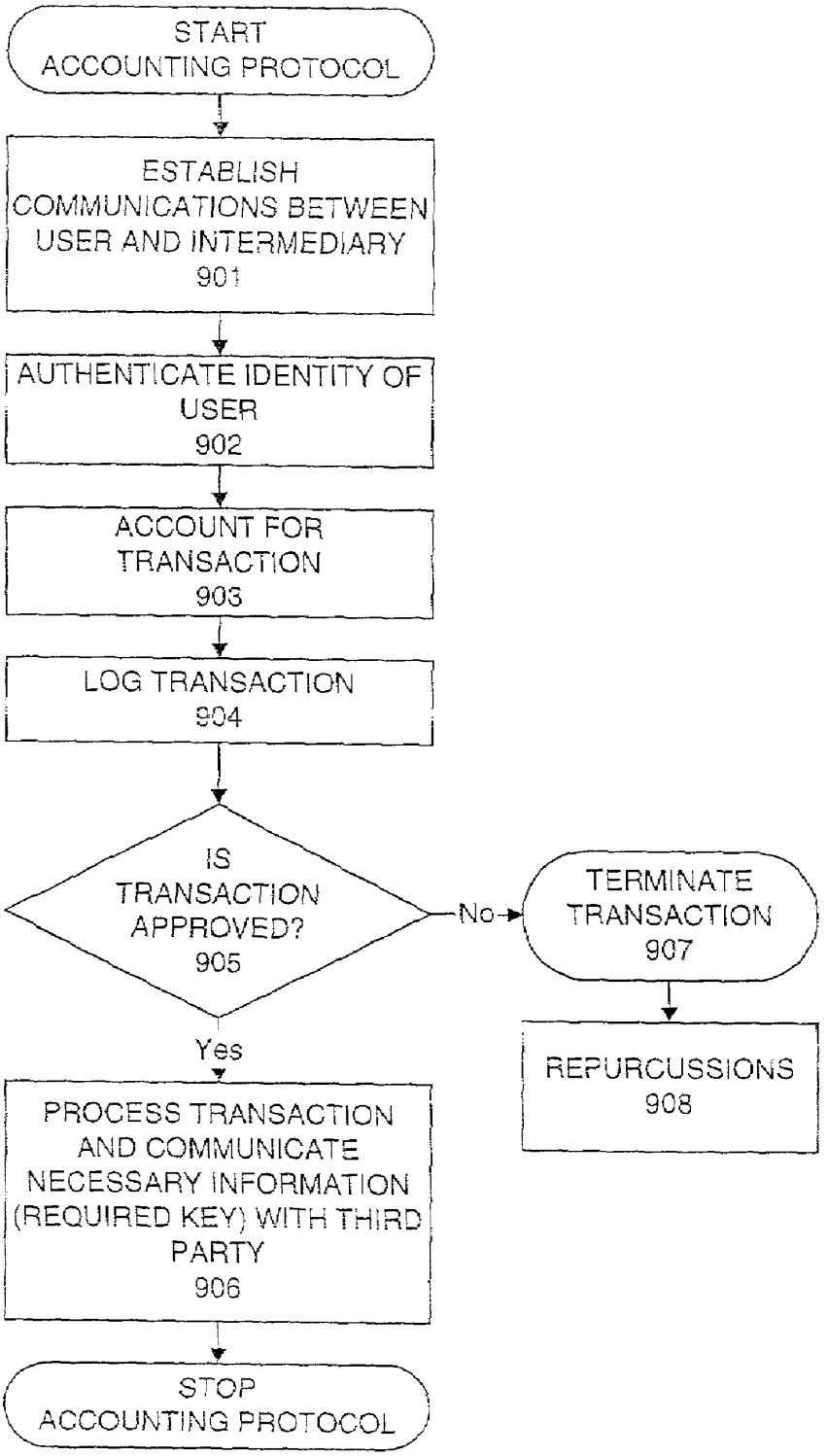

START
ACCOUNTING PROTOCOL
ESTABLISH
COMMUNICATIONS BETWEEN
USER AND INTERMEDIARY
901
AUTHENTICATE IDENTITY OF
USER
902
ACCOUNT FOR
TRANSACTION
903
LOG TRANSACTION
904
IS
TRANSACTION
APPROVED?
905
No
TERMINATE
TRANSACTION
907
REPURCUSSIONS
908
Yes
PROCESS TRANSACTION
AND COMMUNICATE
NECESSARY INFORMATION
(REQUIRED KEY) WITH THIRD
PARTY
906
STOP
ACCOUNTING PROTOCOL

Fig. 9

SYSTEM AND METHOD FOR SECURE THREE-PARTY COMMUNICATIONS

This application claims benefit of priority from U.S. Provisional Patent Application No. 60/278,317, filed Mar. 23, 2001, expressly incorporated herein by reference.

FIELD OF THE INVENTION

The present invention relates to the field of secure communications, and more particularly to multiparty communications supporting transactional accounting.

BACKGROUND OF THE INVENTION

Computer and information system security is currently an important issue. With the proliferation of computers and computer networks into all aspects of business and daily life—financial, medical, education, government, and communications—the concern over secure file access and communications privacy is growing.

Publicly accessible secure database systems pose significant security problems. Attempts to achieve high levels of technical invulnerability may lead to practical problems, system weaknesses and security holes. Passwords may be written near access terminals. Security tokens can be stolen or misplaced. Users may share supposedly secret information. Administration capability bypasses normal security protocols. Secure systems may be built on insecure platforms. Therefore, it is desirable to maintain private information in secure format, without relying on trust of any party who does not require access to the private information, up to a point where it is used by the intended recipient of the information.

The liability or risks involved in holding or communicating private information can well exceed the value of the storage or communications services. Therefore, even in the case of a trusted party, indemnification or insurance may be inefficient or insufficient means for addressing these risks or liabilities. Rather, where considerable risk or liability arises from unauthorized disclosure of the information, the storage or communication of the information must involve an efficient scheme that will minimize the risk of disclosure. Therefore, an intermediary in a transaction preferably handles only encrypted data, and need not be trusted to maintain the privacy of the underlying message. While two-party encryption is well known, schemes are not well developed for providing third party involvement, wherein the third party plays a requisite role in the transaction but which need not or is not trusted with access to the information or the cryptographic key.

A number of communications systems and methods are known for dealing with three-party communications, for example, where a third party provides ancillary services to support the communications, such as authentication, accounting, and key recovery. Often, the nature of these communications protocols places the third party (or group of third parties) in a position of trust, meaning that the third party or parties, without access to additional information, can gain access to private communications or otherwise undermine transactional security or privacy.

Transactions for which third party support may be appropriate include distribution of private medical records, communication of digital content, and anonymous proxy services.

Another aspect of three party communications is that it becomes possible for two (or more) parties to hold portions

of a secret or a key to obtain the secret, without any one party alone being able to access the secret. For example, Silvio Micali has developed a mature Fair Encryption scheme in which a number of trustees collaborate to hold portions of a key used to secure privacy of a communication between two principals, but who must act together to gain access to the secret. In Micali's Fair Encryption scheme, however cooperation of neither of the principal parties to a communication is required in order to access the secret. The third party trustees, as a group, are trusted with a secret. The basis for this trust is an issue of factual investigation. The Micali Fair Encryption scheme does, however, provide a basis for the generation and use of composite asymmetric encryption keys. See, Eyal Kushilevitz, Silvio Micali & Rafael Ostrovsky, "Reducibility and Completeness in Multi-Party Private Computations", Proc. of 35th FOCS, pp. 478–489, 1994, expressly incorporated herein by reference.

The Micali Fair Encryption scheme does not, however, allow communication of a secret in which only one party gains access to the content, and in which the third party or parties and one principal operate only on encrypted or secret information. This system is discussed in further detail below.

See: S. Micali. Fair Public-Key Cryptosystems. Advances in Cryptology—Proceedings of CRYPTO '92 (E. F. Brickell, ed.) Lecture Notes in Computer Science 740, SpringerVerlag (1993) pages 113–138; S Micali, Fair cryptosystems, MIT Technical Report, MIT/LCS/TR-579, November 1993, MIT Laboratory for Computer Science, November 1993.

See also, N. Gilboa, "Two Party RSA Key Generation", Proc of Crypto '99, Lecture Notes in Computer Science, Vol. 1666, Springer-Verlag, pp. 116–129, 1999; D. Boneh, J. Horwitz, "Generating a product of three primes with an unknown factorization", Proc. of the third Algorithmic Number Theory Symposium (ANTS), 1998, pp. 237–251; Lin, Cun-Li, Sun, Hung-Min, and Hwang, Tzonelih, "Three Party Key Exchange: Attacks and a Solution".

Electronic Medical Records

In the field of medical care, accuracy of collected data is of significant importance. Erroneous data, whether collected manually or automatically, presents the possibility of an erroneous diagnosis or treatment. Prior accumulated data about the patient may be relevant to future diagnosis and treatment. Therefore, preservation and availability of accurate medical records remains an important part of the modern health care system.

The art of medical record keeping has developed over centuries of medical practice to provide an accurate account of a patient's medical history. Record keeping in medical practice was developed to help physicians, and other healthcare providers, track and link individual "occurrences" between a patient and a healthcare provider. Each physician/patient encounter may result in a record including notes on the purpose of the visit, the results of physician's examination of the patient, and a record of any drugs prescribed by the physician. If, for example, the patient were referred to another clinic for additional testing, such as a blood analysis, this would form a separate medical encounter, which would also generate information for the medical record.

Over the years, paper medical records have evolved from individual practitioners' informal journals to the current multi-author, medical/legal documents. These paper records serve as the information system on which modern medical practice is based. While the paper-based medical record system has functioned well over many decades of use, it has several shortcomings. First, while a paper-based record

system can adequately support individual patient-physician encounters, it is cumbersome to use as a source of pooled data for large-scale analysis. While the medical data in the paper-based records is substantial, the ability to adequately index, store and retrieve information from the paper-based mechanisms prevents efficient analysis of the data. Thus, paper medical records could be a rich source of information for generating new knowledge about patient care, if the data could be accessed on a large scale. Second, each portion of the paper-based record is generated and kept at the site of the medical service. Hence, the total record is fragmented among many sites. Consequently, access by off-site physicians is less than optimal. The inability to access a complete medical record in a short period of time presents problems both for individual care and group care of patients. Thus, electronic medical records (EMRs) have been developed to facilitate storage, retrieval, communication and use of the valuable patient medical history information, both for the particular patient and for studies of patient populations.

While there have been attempts to develop computer database architectures capable of storing and retrieving medical record information which reconcile physicians' desires for maintaining a format of unstructured medical information with database requirements for highly structured data storage, these systems provide an inadequate infrastructure for the efficient transmission, use and security protection of the data.

Medical information poses significant challenges to knowledge management systems. Medical information presently includes file types including various media types, including numeric data, text, scanned text images, scanned graphic images, sound (e.g., phonocardiography and dictation), high resolution images (radiology) and video (ultrasonic imaging and fluoroscopy).

The medical records for an individual may, over time, grow to multiple megabytes or even gigabytes of data, and advanced medical techniques promise to increase the volume of available data. These records come from a number of different medical service providers, and may be stored in geographically disparate locations. Often, a new medical service provider will seek to review all appropriate previous medical records for a patient. Further, in third party reimbursement situations, the third party payor will seek to review records in connection with billed services. These various data types and associated information storage systems are not standardized, impeding efficiency of sharing and communicating the data.

Medical records often include data that is intensely personal, such as sexual habits, drug abuse, psychological disorders, family histories, genetics, terminal diseases, injuries, and the like. This personal information is revealed to, or generated by, treating medical professionals in an environment that presumes an absolute privilege held by the patient. The adoption of electronic medical record systems should not impair this presumption. Thus, while there are legitimate reasons for transmitting medical information files, such transmission must be secure, limited to appropriate circumstances and to authorized recipients.

Indeed, while the private medical information technically cannot be disclosed without the consent of the patient, since at least the time of Hippocrates, the medical institutions that hold this information guard it jealously. Thus, privacy considerations may make it difficult to obtain collaboration between medical institutions in the ongoing treatment of a patient. While there are important legitimate uses for medical data, there is also a substantial possibility for abuse of the data and the associated trust relationship between patient and medical care provider represented therein. Presently, laws and regulations have been promulgated (but not yet effective) regulating electronic medical records.

The U.S. Supreme Court has reaffirmed that the expectation of privacy of medical data is necessary in order to ensure that patients are not deterred from seeking needed medical care. Disclosure of medical information to non-medical personnel without patient consent was a primary concern of the Court. Ferguson v. City of Charleston, No. 99–936. Argued Oct. 4, 2000—Decided Mar. 21, 2001.

Typically, in a hospital medical information system, information relating to patients in a database is generated and used by users having a variety of roles, including doctors and medical professionals of various specialties, nurses, therapists of various types, paraprofessionals, social workers, clinical laboratories, and bedside devices (which may automatically generate or receive patient information). In addition, medical information is used, but typically not generated by, pharmacies, administrators, lawyers, insurers or payors, and other parties. Because of the many types of caregivers and other data users, the idea of role-based access is appropriate; basically, medical professionals of different types will require access to various subsets of the medical record. For example, typically the primary care physician and certain consults will require full access, while others may not require full access.

One scheme for increasing the portability of medical records is to provide personal data storage devices, for example in credit card format optical storage medium. These devices, however, present a security risk, since it cannot be presumed that the patient will be able to provide consent to the use of the information when required; thus, access controls should contemplate that scenario. Further, the information carrier can be lost, unavailable or stolen.

Encryption Technologies

Encryption technologies, particularly public key encryption systems, seek to minimize some of these weaknesses by reducing the need to share secrets amongst participants to a secure or private communication. Typical public key encryption technologies, however, presume that a pair of communications partners seek to communicate directly between each other, without the optional or mandatory participation of a third party, and, in fact, are designed specifically to exclude third party monitoring. Third parties, however, may offer valuable services to the participants in a communication, but existing protocols for involvement of more than two parties are either inefficient or insecure.

Traditional encryption algorithm schemes rely on use of one or more finite keys which are provided to an algorithm which generates a data string which is apparently random, called pseudorandom, but which can be predicted based on a knowledge of both the algorithm and the key(s), allowing extraction of a superimposed data message. Optimality of an algorithm for a given set of circumstances is based on a number of factors, and therefore many different cryptographic schemes coexist. Essentially, the key should be sufficiently long and stochastic that an extraordinarily long period of time would be necessary to attempt a brute force attack on the algorithm, while only a reasonable amount of time is required to generate keys, encrypt and decrypt messages. In addition, the key should be sufficiently long that observation of pseudorandom (encrypted) datastreams does not permit one to determine the key to the algorithm.

Public Key Encryption is a concept wherein two keys are provided. The keys form a pair, such that a message encrypted with one key of the pair may be decrypted only by

the corresponding key, but knowledge of the public key does not impart effective knowledge of the private key. Typically, one of the keys is made public, while the other remains secret, allowing use for both secure communications and authentication. Communications may include use of multiple key pairs, to provide bilateral security. The public key pair may be self-generated, and therefore a user need not transmit the private key. It must, however, be stored.

The basis for Diffie Hellman and RSA-type public key encryption methods is the large disparity in computational complexity between decrypting the public key created cipher text with the public key encryption private key, which is very rapid and simple to do, and working through the possibilities without the key, which takes a very long time through all known means.

Modern public-key data encryption was originally suggested by Diffie and Hellman, "New Directions In Cryptography," I.E.E.E. Transactions on Information Theory (November 1976) (the disclosure of which is hereby incorporated by reference), and was further developed by Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman: "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM 21(2):120–126 (February 1978) (the disclosure of which is hereby incorporated by reference). See also, U.S. Pat. No. 4,351,982, expressly incorporated herein by reference.

The basic reason for public-key encryption system is to ensure both the security of the information transferred along a data line, and to guarantee the identity of the transmitter and to ensure the inability of a receiver to "forge" a transmission as being one from a subscriber on the data line. Both of these desired results can be accomplished with public-key data encryption without the need to maintain a list of secret keys specific to each subscriber on the data line, and without requiring the periodic physical delivery or the secure electronic transmission of secret keys to the various subscribers on the data line.

According to the Diffie Hellman scheme, two hosts can create and share a secret key without ever communicating the key. Each host receives the "Diffie-Hellman parameters". A prime number, 'p' (larger than 2) and "base", 'g', an integer that is smaller than 'p'. The hosts each secretly generate their own private number, called 'x', which is less than "p−1". The hosts next generate a respective public key, 'y'. They are created with the function: $y=g^x$ Mod p. The two hosts now exchange their respective public keys ('y') and the exchanged numbers are converted into a secret key, 'z' by the following function: $z=y^x$ Mod p. 'z' can now be used as an encryption key in a symmetric encryption scheme. Mathematically, the two hosts should have generated the same value for 'z', since according to mathematical identity theory,

$$z=(g^x \text{ Mod } p)^{x'} \text{Mod } p=(g^{x'} \text{Mod } p)^x \text{ Mod } p.$$

A method of public-key encryption developed by Rivest, Shamir & Adelman, and now generally referred to as RSA, is based upon the use of two extremely large prime numbers which fulfill the criteria for the "trap-door, one-way permutation." Such a permutation function enables the sender to encrypt the message using a non-secret encryption key, but does not permit an eavesdropper to decrypt the message by crypto-analytic techniques within an acceptably long period of time. This is due to the fact that for a composite number composed of the product of two very large prime numbers, the computational time necessary to factor this composite number is unacceptably long. A brute force attack requires a sequence of putative keys to be tested to determine which, if any, is appropriate. Therefore a brute force attack requires a very large number of iterations. The number of iterations increases geometrically with the key bit size, while the normal decryption generally suffers only an arithmetic-type increase in computational complexity.

In the RSA encryption algorithm, the message (represented by a number M) is multiplied by itself (e) times (called "raising (M) to the power (e)"), and the product is then divided by a modulus (n), leaving the remainder as a ciphertext (C): $C=M^e$ mod n. In the decryption operation, a different exponent, (d) is used to convert the ciphertext back into the plain text: $M=C^d$ mod n. The modulus (n) is a composite number, constructed by multiplying two prime numbers, (p) and (q), together: n=p*q. The encryption and decryption exponents, (d) and (e), are related to each other and the modulus (n) in the following way: $d=e^{-1}$ mod ((p−1)(q−1)), or equivalently, d*e=1 mod ((p−1) (q−1)). The RSA ciphertext is thus represented by the expression $C=M^e$ mod n. The associated decryption function is $M=C^d$ mod n. Therefore, $M=C^d \bmod n=(M^e \bmod n)^d \bmod n$, indicating that the original message, encrypted with one key, is retrieved as plain text using the other key. To calculate the decryption key, one must know the numbers (p) and (q) (called the factors) used to calculate the modulus (n).

The RSA Algorithm may be divided, then, into three steps:

(1) key generation: in which the factors of the modulus (n) (the prime numbers (p) and (q)) are chosen and multiplied together to form (n), an encryption exponent (e) is chosen, and the decryption exponent (d) is calculated using (e), (p), and (q).

(2) encryption: in which the message (M) is raised to the power (e), and then reduced modulo (n).

(3) decryption: in which the ciphertext (C) is raised to the power (d), and then reduced modulo (n).

Micali, U.S. Pat. Nos. 6,026,163 and 5,315,658, expressly incorporated herein by reference, teach a number of split key or so-called fair cryptosystems designed to allow a secret key to be distributed to a plurality of trusted entities, such that the encrypted message is protected unless the key portions are divulged by all of the trusted entities. Thus, a secret key may be recovered, through cooperation of a plurality of parties. These methods were applied in three particular fields; law enforcement, business auctions, and financial transactions.

Essentially, the Micali systems provide that the decryption key is split between a number (n) of trusted entities, meeting the following functional criteria: (1) The private key can be reconstructed given knowledge of all n of the pieces held by the plurality of trusted entities; (2) The private key cannot be guessed at all if one only knows less than all (<n−1) of the special pieces; and (3) For i−1, . . . n, the ith special piece can be individually verified to be correct. The special pieces are defined by a simple public algorithm which itself exploits the difficulty in factoring large numbers as a basis for asymmetric security.

SUMMARY OF THE INVENTION

The present invention provides a system, method and business model for conducting transactions involving private information wherein an intermediary performs a requisite function with respect to the transaction without requiring the intermediary to be trusted with respect to the private information or cryptographic keys for communicated information. This system and method employ secure cryptographic schemes, which reduce the risks and liability for

unauthorized disclosure of private information, while maintaining efficient and robust transactions.

The system and method according to the present invention provide a basis for a set of business models, in which the third party accounts for secure data transactions, by maintaining a critical logical function in data communication. Thus, during each such transaction, the intermediary may force or require a financial accounting for the transaction. Further, by exerting this control over the critical function outside the direct communication channel, the intermediary maintains a low communication bandwidth requirement and poses little risk of intrusion on the privacy of the secure communication. Further, the intermediary never possesses sufficient information to unilaterally intercept and decrypt the communication.

The present invention also provides a system and method for providing ancillary services with respect to communicating information. These ancillary services encompass, for example, applying a set of rules governing an information communication transaction. For example, the rules limit access based on recipient authentication, define a financial accounting, role or class of an intended recipient, or establish other limits. These services may also include logging communications or assisting in defining communications counter-parties. The access control is implemented by an intermediary to the underlying transaction, which facilitates the transaction by removing the necessity for a direct and contemporaneous communication with the equitable holder of a pertinent right for each transaction. The intermediary maintains a set of rights-associated rules, over which it may hold legal title. The intermediary serves as a trustee, applying the rules on behalf of the equitable owner of the right. In order to enforce rights-based restrictions, the trustee may hold, associated with the rights information, a key, for example an encryption key, necessary for access or use of the information. This arrangement is termed herein a Virtual Trust, and the intermediary is therefore a termed Virtual Trustee.

According to the present invention, the Virtual Trustee is trusted to implement the rules, but not necessarily trusted with access to, or direct and sole access control over the information. According to a preferred embodiment, the Virtual Trustee, acting alone, cannot access or eavesdrop on the private information or a communication stream including the information. Further, in accordance with the Micali split key escrow scheme, the Virtual Trustee may be implemented as a set of entities, each holding a portion of a required key.

The present invention also provides enhancements to traditional secure communications by providing involvement of a third party, or intermediary, who need not, and preferably does not, have access to the communicated information, while providing transaction-support services between the two parties involved in the communication. According to a further embodiment of the invention, only one party to the communication is privy to the secured information; the host for transmission of the information does not, as a part of the transaction, access the information itself.

Thus, the system according to the present invention provides a conduit for the authorized transmission of records, such as medical records, while maintaining the security of the records against unauthorized access. A preferred communications network is the Internet, a global interconnected set of public access networks, employing standardized protocols. Thus, the records may be transmitted virtually anywhere on earth using a single infrastructure. Alternately, private networks or virtual private networks may be employed. In fact, as the system according to the present invention gains ubiquity, a private network model would be preferred, in order to increase security and allow the system to be tuned to the types of data and quality of service demands made by users.

An embodiment of the present invention involves the implementation and use of a Virtual Trust, wherein an owner of rights in information entrusts the application of a set of rules and/or limitations, to a Virtual Trustee. The Virtual Trustee implements these rules and/or limitations, unless countermanded. One of the rules and/or limitations may be to seek input from the rights owner, if available.

According to one embodiment of the invention, a user provides to the intermediary necessary transactional information relating to private information, in a manner that discloses little or no private information to the intermediary. In like manner, private information may be supplied to a user after the user has supplied necessary transactional information to the intermediary, without in the process disclosing the private information to the intermediary. These techniques may be extended to allow personally identifying information to be removed from a communication by substitution with a non-personally identifying code, supplied by the intermediary. Again, this anonymous process may take place without providing the intermediary with the private information.

In some embodiments, the two principals to the communication remain anonymous with respect to each other, while in other instances, they are known to each other. In the former case, a proxy is provided to avoid divulging the address (e.g., logical or physical address) of the recipient, and, depending on communication protocol, the identity of the sender. The communication channel may remain secure between the two principals, although the proxy becomes trusted with respect to identities of the principals.

The intermediary may, as a matter of course, in the course of its duties, implement a set of rules on behalf of a rights-holder for the information, and indeed communications structures and protocols may be established to force a critical portion of each subject communication to pass through the intermediary.

Different rules may be applied, for example, based on the nature of the information, the role of the recipient, context of the information request, and preferences of a rights-holder of the information.

In a medical embodiment, a patient may, within the scope of available resources, define rules and procedures for access to his or her own medical records. Thus, the rules defined by a patient or record owner may differ from those imposed by the repository medical institution. A default set of rules may be provided which restricts access to medical professionals who can demonstrate authorization, with disclosure of particular transactional records limited according to the requestor's role or other set of rules. As trustee or agent for the patient, the intermediary may also implement more or less restrictive rules as defined by the patient, and release records accordingly. The intermediary may also implement a set of rules defined by the respective custodian medical institution in connection with its own internal processing or communications.

Presently, medical records typically include information that is integral with a physical embodiment. For example radiological records are integrated into the film. The original medical record, embodied in its physical manifestation, is "owned" by the originating institution or provider, subject to access control and copying requests by the patient. See, DeWitt et al, "Patient Information and Confidentiality",

Treatise on Health Care Law, 16.01 (Kaufman et al., Eds., 1998). However, as electronic medical records gain prominence, and the physical manifestation of the medical records is transformed into information stored in a computer storage device, the medical record may ultimately be treated as property of the patient, subject to retention of a non-distributable (or otherwise subject to limited rights) copy by the originating institution or provider. The present invention therefore provides a system through which a patient may exert various incidents of ownership over the electronic medical record, including access control, copying, retention, and accounting therefore. According to the present invention, this control may be exercised by entrusting the encryption key(s) for the electronic medical record with an intermediary, who acts under the direction and authority of the patient.

The present invention also encompasses monetary transactions involving the information usage and/or communication. According to one embodiment, digital signatures may be employed in monetary transactions that, after authentication, become anonymous. Thus, according to the present invention, a personally identifying digital signature may be substituted by the intermediary with an anonymous transaction or session identifier. In this case, while the transaction becomes anonymous, it is not necessary for the intermediary to be a direct party to the exchange of value between the principals involved in the communication, and thus the intermediary does not necessarily become privy to the exchange details.

According to the present invention, the security and privacy scheme of the present invention may be employed to convey content to users while ensuring compensation for rights-holders in the content.

According to the present invention, an architecture is provided which allows accounting and implementation of various rules and limits on communications between two parties. Further, an intermediary becomes a necessary part of the negotiation for communication, and thus has opportunity to apply the rules and limits.

Traditionally, medical records maintenance and upkeep have imposed a significant cost and burden. While enterprises have evolved for outsourcing of certain functions, these enterprises have not directly represented the interests of the patient, and rather serve as agents for the medical record custodian.

According to one embodiment of the present invention, each use of a record may trigger an accounting/audit event, thus allowing finely granular transactional records, which may reduce the risks of security and privacy breach in connection with record transmission. Importantly, the present invention allows usage based financial accounting for the information, imposing a financial burden according to a value and/or consumption of system resources. For example, the cost to a user could be a flat fee, depend on a number of factors, be automatically calculated, or relate to volume of usage.

The accounting may also compensate a target of an electronic message for receipt thereof. Thus, a marketer may seek to send an advertisement to a user. The user may then compel the marketer to send the electronic message through an intermediary, providing compensation to the user.

In establishing a secure communications session between the user and the intermediary, it may be useful in some circumstances to employ a challenge-response authentication scheme, for example by passing messages back and forth between the user and the intermediary, the user and the data repository, or the data repository and the intermediary.

According to the present invention, the user's "role" may be checked for consistency with a set of role-based usage rules. The reported role may be accepted, or verified with resort to an authentication database. Based on the role of the user and the identification of the content, the authority of the user to receive records may be determined.

In one embodiment, a user is required to identify the specific records sought, and therefore the authorization matrix representing correspondence of record content and user role may be associated with each record, and may be verified by the data repository as a part of a local authentication process prior to transmitting any portion of a record. Thus, the matrix may represent a metadata format describing the content of the record and the level or type of authority of the user to access that record. This metadata may, of course, itself be privileged information.

In the event that the distribution of metadata or its application at a site is impermissible, a separate metadata processing facility may be provided. This facility may process the metadata in an anonymous index format, thus reducing or eliminating the risks or a privacy or security breach. The user authority matrix may be protected using the composite session key format according to the present invention, and therefore made secure even from the intermediary, which, in this case, may communicate the authority matrix and transactional request details to the metadata processing facility using a composite of a user session key and a metadata session key. The results of the authorization may be transmitted directly from the metadata processing facility directly to the data repository, in the form of a prefiltered specific record request. The intermediary may account for the transaction either on a request-made basis, or communicate accounting information with the data repository, for example to properly exchange required keys and complete the transaction.

The record indices may thus be maintained by entities privy to private information, with results returned to the user, without requiring any disclosure to the intermediary, or maintained by entities insulated from an association between a complete identification of the metadata and the content thereof. Preferably, the index entry for a record includes an identification of the location of the content record and a set of access rules, which are, for example, role based. Alternately, the intermediary may maintain the index locally and apply the respective rules.

The role-based access rules are generally defined automatically, and may be based on contextual and circumstantial data. Manual rules and edits may also be supported. Typically, a hierarchy is defined of data sensitivity, with the most sensitive data provided with the highest level of restrictions. Typically, primary care providers have the highest level of access, while paraprofessionals and other support personnel have data on a context-dependent requirements basis only. Further, non-professionals may be provided with data on a need-to-know basis only.

Other medical personnel have access to the record based on context and role. For example, a respiratory therapist might require access to pulmonary and central vascular history records, as well as to abstracts of acute medical information, current pharmaceutical information, scheduling (e.g., for inpatient care), and specific notes directed to the therapist, individually or as a part of a treatment group.

Thus, a past history of depression (resolved) in a patient admitted for a kidney stone would likely be communicated only to the primary care physician and psychiatric treating professional if any. Possibly, this data would be communicated to a pain management professional, if the past history

of depression had a pharmacological or drug abuse component. A surgical consultant, however, may be provided with the entire record. This data may also be deemed contextually irrelevant to the acute treatment.

For example, a treating physician, an oncologist, may seek, on behalf of a lung cancer patient, all radiologic studies of the chest over the past three months, as well as non-radiologic hospitalization records over the past three years and summary notes of other medical or surgical consultations or treatments over three years. The request, as well as a role-based identification of the oncologist, are relayed to the intermediary, which may process this data internally, or relay it to a separate entity for processing. In the latter case, the information may be completely blinded, according to the present invention, from the intermediary. Initially, the instructions of the patient are recalled from a database, to indicate any specific or general restrictions placed on the release of data. An exemplary role-based access authentication would determine that a primary treating oncologist is indeed authorized to receive radiological (chest) and recent hospitalization records. Further, the indices for the medical summary notes could be screened for pertinence criteria. Thus, information relating to a drug abuse rehabilitation center visit might be restricted upon request of the patient to mental health professionals. In this case, such private information could be screened from the oncologist, likely with some indication of the restriction, allowing the oncologist to subsequently request authorization from the patient. If, on the other hand, the requesting professional was a nurse, the indication of restricted information might not appear, since this indication itself might be deemed a disclosure and the apparent need is lower.

In order to provide further security for the records and the use of the system, various techniques are available. For example, dummy content records may be added to the database and index therefore. Any access of these records is presumably based on an attempt for unauthorized access. Thus, the existence of these records, with access tracking, allows detection of some unauthorized uses of the system. Another method of securing the system is the use of steganographic techniques, for example embedding watermarks in audio and images, pseudorandom dot patterns in scanned page images, random insertion of spaces between words, formatting information, or the like, in text records. Therefore, records obtained through the system may be identified by their characteristic markings. In fact, every authorized record may be subjected to a different set of markings, allowing a record to be tracked from original authorized access to ultimate disposition. An explicit bar code, watermark or other type of code may also be provided on the document for this purpose. It is noted that such markings cannot be implemented on encrypted data at the point of transmission, and thus this type of security requires access to the raw content. However, this may be implemented at the point of decryption, which may be in a sufficiently secure environment. For example, a secure applet may be provided, employing a securely delivered session key, which processes records to test for existing watermarks and to add or substitute a new watermark. Thus, the present invention provides a system for the decryption and watermarking of data, in a content (or content type)-specific manner. An online handshaking event may occur on decryption, to provide confirmation of the process, and indeed may also authenticate the user of the system during decryption.

According to the present invention, asymmetric key encryption may be employed to provide the establishment of secure communications channels involving an intermediary, without making the intermediary privy to the decryption key or the message. Thus, by transmitting only relatively unprivileged information, such as respective public keys, the information and integrity of the system remains fairly secure.

In order to provide a three party transaction in which the intermediary is a necessary party, the information sought to be transmitted is subjected to a secret incomprehension function (e.g., a cryptographic or steganographic function) with the key known only to the intermediary. In establishing the communication channel, the information is transcoded between a first comprehension function and a second comprehension function without ever being publicly available.

Modulo arithmetic is both additive and multiplicative, thus, using the same modulo n:

$$(A^x \bmod n \cdot A^y \bmod n) \bmod n = A^{x+y} \bmod n;$$

$$((A) \bmod n + (B) \bmod n) \bmod n = (A+B) \bmod n.$$

$$((A) \bmod n \cdot (B) \bmod n) \bmod n = (A \cdot B) \bmod n.$$

$$(A^x \bmod n)^y \bmod n = (A^y \bmod n)^x \bmod n = A^{xy} \bmod n$$

A preferred algorithm according to the present invention relies on the multiplicative property of modulo arithmetic; in other words, A mod B*C mod B=(A*C) mod B. However, this property is not "reversible", in that knowledge of (A*C) mod B and either A or C does not yield the other, unless the product A*C is less than B, since the modulo function always limits the operand to be less than the modulus value.

Thus, it is seen that in an RSA scheme, $M=C^d \bmod n=(M^e \bmod n)^d \bmod n$. Therefore, in order to communicate the intermediary private information to the intended recipient, the recipient public key 'e1' and intermediary private key 'd2' are defined using the same modulus n, multiplied, and provided to the sender. At the sender, the ciphertext $C2=M^{e2}$ Mod n, previously encrypted with the intermediary's public key e2, is subjected to the function: $C1=C2^{d2e1} \bmod n=M^{e1} \bmod n$. The recipient may then apply its private key d1 to decrypt the message: $M=C1^{d1} \bmod n$.

It should be understood that the algorithm described herein represents merely a portion of an RSA-type public key infrastructure, and that generally all known techniques for preparing the message, maintaining a public key directory, and the like, may be employed in conjunction therewith, to the extent not inconsistent. Thus, the transcoding algorithm should be considered as a generally interchangeable part of the entire cryptographic system, which may be substituted in various known techniques, to achieve the advantages recited herein. In general, only small changes will be necessary to the systems, for example, accommodating the larger composite key length. It is also particularly noted that there are a number of known barriers to exploits that are advantageously employed to improve and maintain the security of the present system and method.

See, David Chaum, "Blind Signatures for Untraceable Payments", Proceedings of Crypto 82, August 1982, p. 199–203. According to the Chaum scheme, a server assists a user in decrypting a message without releasing its secret Key or gaining access to the encrypted message. The user communicates a symmetric function of the ciphertext to the server, which is then processed with the secret key, and the resulting modified ciphertext returned to the user for application of an inverse to the symmetric function. See, U.S. Pat. No. 6,192,472, expressly incorporated herein by reference. This technique, however, requires a communication of the complete message in various encrypted forms to and from

the server, a potentially burdensome and inefficient task, and is not adapted to communicate a secret file from a first party to a second party.

According to an embodiment of the present invention, a source privy to the communication employs a public key encryption paradigm to require that for comprehension of an encrypted message, at least two keys are required, with all of the predefined keys being required to decrypt the message, and with no apparent relation between the keys, making prediction of one key part difficult or impossible based on the corresponding other key part(s) and the ciphertext message. Thus, at least three parties must cooperate to transmit a message, the sender, the recipient, and a third party holding a necessary key part. This results in an ability to audit and log communications without giving access to confidential information to the auditor. This also facilitates economic transactions, since the communication of the missing key information provides an opportunity for a mandatory third party accounting.

According to the present invention, the holders of key parts are not equal parties to the transaction. Rather, one party acts as the intended recipient, who must "procure" the remaining private key parts in order to use the information. This procedure allows the entity that transmits the information to be assured that the transmission will be secure, even with respect to a trusted third party, while ensuring that the intended recipient must cooperate with the intended third party. For example, the third party receives a fee or other value for this interaction, and is able to log the identity of the intended recipient and time of the transaction. In many instances, for example access to medical information, this allows a third party to authenticate information requests, apply access rules, and log transactions, on behalf of patients or medical institutions, without itself handling the sensitive information. The health care institution, on the other hand, can achieve compliance with regulations protecting the privacy of medical records while providing portability thereof, without increasing its staff or breaching security protocols. Patients, meanwhile, employ a third party for authenticating requests for medical information, logging access, and implementing various rules and limitations.

Using this scheme, the original ciphertext encryption key and recipient private key need never be disclosed, and thus may each be retained for use over an extended period. The session encryption key, however, will vary with each message.

It is noted that, since the intermediary holds the decryption key for the record, it may, in exceptional circumstances and in cooperation with the repository, decrypt the plaintext message. Therefore, it is seen that, even if a user fails to comply with the required access rules (one of which may be, for example, the express consent of the patient), desired information is not lost, locked or completely unavailable. Rather, the trustee may be given the discretion to release the records or to request release of the records during an emergency.

The present system thus may be used in a number of areas. For example, it may be used to transmit confidential medical records through a public network. The (not yet effective) regulations issued pursuant to the Health Insurance Portability and Accountability Act (HIPAA) require that patient medical information be securely transmitted, that access be logged, and that the identity of the recipient be authenticated. However, while secure transmission is relatively easy to perform using modern computing architectures, the logging and authentication require a substantial infrastructure and overhead to maintain. Many institutions would be quite burdened by supporting such potentially labor intensive and infrastructure intensive obligations. Therefore, the present system allows secure access to an institutional database, with the logging and authentication potentially outsourced, to an intermediary. The outside organization, in this case, implements the required security protocols to assure patient data confidentiality both inside and outside the medical institution. The data repository for the medical information may encompass only encrypted information, and therefore implementing an appropriate communications firewall for controlling public access of the database is facilitated.

A trusted entity may control external access to an institutional database. This trusted entity may also control internal access and logging in like manner. In like manner, the trusted entity may also perform inter-institutional functions, for example where portions of a patient medical record are housed in various institutions. According to the present invention, the degree of trust required of an intermediary may be less than that required of either a key escrow agent or a repository with complete access to the private information. While the intermediary entity may have access to certain tertiary medical record information, such as the existence of records and identity of those accessing the records, the primary records may remain secret, even with respect to this intermediary entity. The intermediary system may incorporate a directory of patient records, assisting an authorized user in obtaining various records.

It is noted that, while medical records are retained by a custodial institution, the corresponding patient retains important rights therein. Thus, the present system may be expanded to provide the patient with a key portion, which is also required for access to the records. In this case, since the patient's consent will not always be available in a timely manner when the record is needed, a key escrow or key recovery scheme may be implemented to obtain this key portion. This may be implemented in known manner, but preferably it is maintained by the trusted entity, since this will make any such recovery transaction more efficient.

In order to increase portability, physical records, especially archives, may be stored physically or logically outside the source institution. Thus, limitations of access and bandwidth imposed by a public network gateway for an institution do not impede information transfer. Authorizations, as distinct from the information sought to be communicated, are verified on-line, and may involve access to the source institution, but typically command substantially lower bandwidth requirements.

Current medical records are subject to at least two important controls exerted by the patient: The patient can restrict access to the record, and the patient may demand access and a copy of the record. These two rights, together very much define a type of property interest. Since the trusted entity acts as a gatekeeper to the records, it may also act as an agent or trustee for the patient, exercising access rules and the like, by way of the required keys. Thus, it may be considered that the key(s) and possibly other data are held by the trusted entity is in trust for the patient. The intermediary may adopt a business model either directed to serving the needs of the medical institution(s), the patients, or both.

The trust model for the access privileges allows the trustee the legal authority to act on behalf of the beneficiary (in accordance with the authority granted at the time the trust was created or in effect at the time of the access request). In the case of medical records the beneficiary is the patient. Further, the trust model creates a framework in which courts may provide guidance and/or mandate to a trustee. Thus, in contrast to a typical contractual relationship, the trustee of

the access rights to the medical records stands in a different position than a mere party to a contract.

In alliance with this trust model, the intermediary is in a unique position to act as a health care proxy and an executor of a living will for patients. In this model, the patient provides a living will or other instructions to the intermediary. When the patient is unavailable and a decision must be made, the intermediary can search its database for a most current instruction or rule authorized by the patient, and provide an authenticated communication to the health care provider communicating the patient's wishes. For this service, the intermediary may charge a fee, for example a yearly maintenance fee, a per transaction fee, and/or statutory or court-awarded fees.

A potentially significant use of existing medical records is in conjunction with a data mining system. This is because it is generally considered quite expensive to capture medical records, remove patient-specific identification, and place the resulting anonymous records in a database. On the other hand, as the use of electronic medical records and intelligent means for extracting anonymous data from medical records grows, this data will become more accessible. The present system provides an infrastructure for amassing, maintaining and exploiting the value of this data. Thus, by filtering data, obtaining filtered data, or hosting an index to anonymous data, the present intermediary provides a resource to facilitate use of medical data. For example, third party payors may seek to determine the standard of care or best practices for a given patient, in the context of authorization of payment for a procedure. Likewise, a health care professional may seek to determine a patient prognosis. By providing an accessible system that links data for a specific patient, with anonymous data for a plurality of patients with potentially similar medical issues, significant efficiencies may result. Such a system including anonymous data could be established separately from the private medical record database system. The intermediary system according to the present invention may provide authentication and accounting system for the use of such anonymous data, as well.

The intermediary may receive fees from or be compensated by the user, by the data repository (e.g., the medical institution or provider), by the patient, or by a third party payor (e.g., an insurance company, health maintenance organization, government entity, etc.) or a combination or subcombination thereof. The intermediary may therefore negotiate for access to the database prior to granting authority.

Another application for the intermediary system for distributing the encryption key lies in the entertainment industry. In particular many forms of entertainment, including music, videos, and the like, involve massive data files, ranging from about 500 kB to multiple gigabytes of data.

One solution proposed for the delivery of such data streams is called a peer-to-peer architecture, wherein the hosting of information is distributed over the population of users of the information. Thus, any user seeking information can communicate with another user (or a set of users) seeking to transfer the information. Since the Internet provides a highly redundant and distributed communications network, the capacity of the network is large and the incremental cost of adding a new work to the distributed database is low.

However, typically, the owners of entertainment works seek to maintain control over use of the works and seek to receive compensation for their transfer and/or use. Therefore, the present system allows the work to be locked or encrypted, wherein the owner of the work or its agent serves as a required third party to the communication, and provides the recipient with a dedicated decryption key for use of the work upon accounting therefore. Thus, the recipient is not dependent on a single connection to a host server to obtain the work, and the owner of the work need not invest in maintaining massive file server. This reduces the transaction and infrastructure costs to the owner, which are generally a high percentage of the overall costs in the delivery of electronic media programs. The system may also provide compensation to the host (repository) for allowing use of its resources.

The system operates as follows. Each user is provided with a customized application that manages local files. Each local file is registered with an external server. A user seeking to obtain a copy of a file queries the external server to find appropriate copies residing on the network. Either automatically or manually, the requesting user initiates a transfer of the file through a communications link from another "peer" user. This communication is encrypted, so that no eavesdropper can misappropriate the file, and the intended recipient accounts for its receipt. The decryption key is defined such that a portion is dependent on the identity of the recipient, and a portion provided by or on behalf of the owner of the content. This latter key portion is typically provided only after an accounting, such as a payment for the use of the file. The host for the file encrypts the file using a public key or set of public keys for the recipient and owner. These keys, of course, may be the respective trustee keys defined by Micali, or according to another appropriate encryption scheme. The host for the content may be compensated for use of its system, thus encouraging use within the rules of the system, rather than circumventing the system.

According to one embodiment, in order to prevent users from circumventing the system, the user's public key, and/or the owner's key, may also be embedded as part of a watermark or embedded signal that must match a user's access system. When the embedded data matches, the system operates normally. In the case of a mismatch, it will not operate. The application software at the host converts the embedded signal between that user's and the new user's. In order to prevent circumvention, each user system may periodically report to the intermediary its own "serial number" and possibly the file usage. A user credit card or other financial guaranty may also be used to automatically compensate for any usage.

The present invention allows for the distribution of data from a repository, which does not require the repository to be trusted with the data. Thus, encrypted data may be transmitted, replicated, and cached to the benefit of an owner of rights in the data, since the data is not usable without an encryption key. Such data may be, for example, consumer media or multimedia works, which advantageously are subject to caching by edge servers for efficient utilization. According to the present invention, and in contrast with prior methods, in order for a data record to be used, a separate accounting and authentication transaction is required, and the data record transmitted to the user is presented in a format that requires a custom-generated cryptographic key. Thus, the data remains secure during archival storage and transmission. In order to limit the ability of an authorized recipient from retransmitting the record data, the data may be "fingerprinted" or watermarked to the user or its computing hardware based on the transcryption operation at the data repository (or remote key handler, if present). This fingerprinting allows either track-

ing of unauthorized transmission, or preventing the use of the record data on different systems or by different users.

As used herein, the phrase "comprehension functions" encompasses both cryptography and steganography. Thus, secret information is required in each case in order to comprehend certain information. In the former case, the information is scrambled, and must be decrypted, while in the later case, it is hidden, and must be located. It is, of course, possible to combine the techniques and employ hidden and scrambled messages, it is also noted that, in some instances, it is not necessary to apply a comprehension function to all of a the information in a message. For example, in the case of medical data, it is often the maintenance of security of personally identifying aspects that is sought. Therefore, often only the personally identifying information needs to be selectively obscured. Likewise, in the case of entertainment media, it is possible to selectively degrade the information by selecting only a portion of the media information to selectively obscure, which makes the resulting information significantly less valuable. By selectively applying such a comprehension function only to a portion of the information, substantial computational resources may be conserved or spared.

According to another embodiment of the invention, the transcryption scheme according to the present invention may be employed to securely communicate cryptographic codes between parties to a communication, for example a symmetric encryption key. For example, the Advanced Encryption Standard (AES) employs the Rijndael algorithm, which may provide highly efficient encryption and decryption. Thus, the asymmetric key encryption may be directed principally toward key exchange.

According to another embodiment of the invention, an encrypted message (ciphertext) is "transcoded" from a first encryption type to a second encryption type, without ever passing through a state where it exists as a plaintext message. Thus, for example, an intermediary to the transaction who negotiates the transaction, need not be privileged to the information transferred during the transaction. In the case of medical records, therefore, this means that the intermediary need not be "trusted" with respect to this information.

A preferred embodiment of the invention provides composite key asymmetric cryptographic algorithms to, among other advantages, avoid revealing a plaintext message during intermediate processing. However, it is also possible to employ symmetric key cryptography, especially since the remote key handler is a privileged environment, and may be provided with sufficient security to abate the risk of message disclosure. Further, in some embodiments, the system risks attendant in releasing both the permanent encryption key along with the ciphertext are insubstantial, and therefore a transcoding or transcryption process is not required. These various embodiments are encompassed by the present invention.

As an example of the algorithm according to the present invention,

p=61 and q=53,n=pq=3233.

(e*d)=1 mod((p−1)(q−1))

choosing e1=23 results in d1=407;

choosing e2=101, d2=1421.

Selecting an arbitrary message text 1111, the function $C=M^{e1d2}$ mod n results in the equation:

$$C=(1111)^{23*1421} \bmod (3233)=2758 \bmod (3233).$$

To invert this encryption with ciphertext 2758, $M=C^{e2.d1}$ mod n, resulting in the equation:

$$M=(2758)^{101*407} \bmod (3233)=1111.$$

Thus, it is seen that a preferred algorithm according to the present invention is operative to encrypt and decrypt the message, with a composite key that is relatively large, and thus difficult to determine the respective factors.

A system embodiment of the invention using the preferred algorithm has three properties of particular relevance: (a) while an intermediary may be a necessary party to the transaction, the protocol does not provide the intermediary with sufficient information to eavesdrop, thus, the intermediary is not trusted with the secret communication; (b) due to the transcryption, the sender of the message may maintain an encrypted repository, and also need not be trusted with the secret communication; and (c) that neither the decryption key for the message, nor the message, is transmitted at any stage in the process in an analytic form. Therefore, the message is provided only to an authorized and actively authenticated recipient.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** shows a block diagram of a first embodiment of the communications system according to the present invention;

FIG. **2** shows a block diagram of a second embodiment of the communications system according to the present invention;

FIG. **3** shows an idealized representation of a three party communication transaction according to the present invention;

FIGS. **4**A and **4**B show workflow diagrams for the input and output of encrypted records according to the present invention;

FIG. **5** shows a flowchart of the actions of the user during typical transactions according to the present invention;

FIG. **6** shows a flowchart of the actions of the intermediary during typical transactions according to the present invention;

FIG. **7** shows a flowchart of the actions of a third party to the transaction according to the present invention;

FIG. **8** shows a flowchart of the actions of the remote key handler according to the present invention; and

FIG. **9** provides a flowchart of an accounting protocol according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention provides a transaction scheme involving at least three parties for communication of a message, in which all parties are required, yet only one party. e.g., the intended recipient or user, is trusted with the message.

The following identities characterize the known RSA algorithm: $C=M^e$ mod n and $M=C^d$ mod n. For the complete transformation, the relationship is as follows: $M=C^d$ mod $n=(M^e)^d$ mod n. According to the present invention, it is desired to transform ciphertext 1 (C1) into ciphertext 2 (C2), in a secure manner without ever revealing the plaintext message during the process. In order to achieve this transformation from C1 to C2, the two-step process is consolidated. Thus, the decryption according to a first decryption key $M=C1^{d1}$ mod n and the reencryption according to a second decryption key $C2=M^{e2}$ mod n are combined into a single transcryption operation, $C1^{d1e2}$ mod $n=M^{e2}$ mod

n=C2. So long as the factors of d1·e2 remain secret, it is infeasible to factor thus number, and thus this transformation inherits the advantages of the RSA encryption scheme. Thus, the plaintext message remains secure through this transformation. In fact, because the transformation is integral, relatively low security is required for the starting and transformed ciphertext, and the crypto-processor itself.

This process also lends itself to three (or more) party transactions, wherein each party is a required participant (maintains secret information necessary for the communication) but only an intended recipient (user) has access to the plaintext message.

Accordingly, if a transaction intermediary supplies a transcoding or transcryption key to the message repository, comprising at least two secret components (so that the composite key may not be factored), an existing ciphertext may be transformed into a new ciphertext. While the components of the composite transcode key are secret, due to the nature of public key systems, these are insufficient for the intermediary to gain access to the message. The two secret components include a key specific for the user, and a key specific for the existing encryption of the message ciphertext. The resulting transformed ciphertext is therefore a public key encrypted message for the user, which can only be decrypted with the user's private key. In order to maintain the security of the original message against subsequent uses, it is preferred that the user's public key-private key pair be a session key, that is, accounted for and used only for the single transmission and subsequently discarded. The "public" portion of the session key pair is transmitted by the user to the intermediary, which is held in secrecy and multiplied by the private key for the existing ciphertext message. In this way, the intermediary has no knowledge of the "private" session key, and cannot itself intercept the communication.

Thus, the data repository handles only encrypted messages according to the present scheme. The decryption key for these messages is held secretly by the intermediary only, and neither released nor transmitted in a form subject to decomposition.

The intermediary, while holding a sufficient decryption key, has no access to the repository ciphertext message, which is separately maintained by the repository.

The user receives a ciphertext message, which is decrypted with a secret key. Typically, the repository will further encrypt the transmission to the user with a permanent-type public key for that user, which will be obtained from or verified by a separate certification authority. Thus, even if the intermediary were to employ a dummy key, the resulting transmission from the repository would still be secure with respect to the intermediary.

In operation, the user generates on a session basis, a key pair, and provides one portion to the intermediary, the other is maintained in secrecy for the duration of the transaction. The intermediary receives the session key and multiplies it with the secret decryption key for the message held by the data repository. Both the session key and the decryption key individually are held in secrecy by the intermediary. The data repository further receives from the intermediary an identification of the user, which is used to query a certification authority for an appropriate public key. The data repository "transcrypts" the encrypted message with a composite key (resulting from the multiplicative combination of the Record Private Key, the User Public Session Key and the Intermediary Private Session Key) as well as the User (persistent) Public Key to yield a new encrypted message, which is transmitted to the user. The user then applies the retained portion of the session key, as well as its persistent private key, resulting in the original plaintext message Likewise, the composite encryption key used by the data repository results from the combination of the Record Public Key. Intermediary Private Session Key, and User Public Session Key.

When data is added to the Encrypted Record Database, it may be advantageous to provide the user with a confirmation comprising a hash function performed on the received data, either in its Composite Session Key format (allowing immediate verification by the user) or in its Record Key format (allowing persistent verification of the transaction), or both. Further, it may also be advantageous for the intermediary to receive or act as conduit for these verification communications, allowing an accounting to take place on such confirmation.

When data is communicated from the Encrypted Record Database to a user, it may likewise be advantageous to provide the data repository with a confirmation comprising a hash function performed on data received by the user. This confirmation may advantageously be communicated through the intermediary, allowing an accounting to take place on such confirmation.

Example 1

The transactional details are now described with respect to FIG. **1**. While there are three particular parties to the process, the User **20**, the Data Repository **30**, and the Intermediary **10**, a fourth party, a Certification Authority **40** is also generally involved. It is also noted that, while the process shown in FIG. **1** generally provides a communication flow of information from the Data Repository **30** to the User **20**, this communication stream may also be reversed, allowing the User **20** to upload information to the Encrypted Database **31** of the Data Repository **30**, using a set of User **20** and Intermediary **10** Session Keys and the User **20** Persistent Private Key. At the Remote Key Handler **33**, the encrypted message is transcrypted with the Record Public Key, securely supplied by the Intermediary **10** through a virtual private network (VPN)-type arrangement, passing through the Data Repository **30**.

The User **20** initiates the transaction by contacting the Intermediary **10**, which typically maintains an Accounting Database **11**, a transaction log **12**, an Authentication Database **13**, and a Secure Private Key Database **14**. The accounting function is typically a financial transaction, wherein the User **20** pays for the information requested. Other forms of accounting are also possible and indeed, the User **20** may be paid for its review of the information. Particulars of each transaction are typically recorded in the Transaction Log **12**, which may be used for auditing, reconciliation, verification, trend analysis, or other purposes. This log potentially allows subsequent aspects of a transaction to be anonymous, with the identifier of the User **20** stripped, while verification of authenticity may continue to be assured through use of an authentication token **23**.

The Authentication Database **13** may, for example, provide a means for definitively identifying the User **20**, and/or, in the case of a medical record, the identity of the patient who consults the User **20**, who is, for example, a health care professional. This identification may be based on a Public Key Infrastructure, biometric identifiers, passwords and/or personal identification numbers (PIN), or other known means. The Intermediary **10** may therefore provide a persistent association of the User **20** and/or a patient in its records, which facilitates accounting, application of rules, recalling of data from a database, etc.

Advantageously, a medical patient may employ a public key to identify himself or herself. This public key is then received by the User **20** as partial evidence of authority and association with the patient. Such keys may expire periodically, preventing persisting use of outdated keys. The Intermediary **10** may then partially authenticate the User **20**, by analysis of the patient public key-signed transmission from the User **20** with respect to a patient private key retained by the Intermediary **10**. In some implementations of the invention, a patient-specific key pair may be used generally as a Record Encryption Key (e.g., the Record Public Key) for records belonging to that patient in the Encrypted Record Database **31**. Generally, this key pair is not identical to the patient key pair used for digital signatures by that patient. It is noted that the Record Public and Private Keys stored in the Secure Record Key Database **14** may, but need not be individually generated for each record added to the Encrypted Record Database **31**, and in fact may advantageously be aggregated and a single set of Record Keys used for a single patient or a group of records relating to the same patient, such as a single hospital admission.

The User **20** typically authenticates itself with the Intermediary **10**, although in certain instances anonymous or semi-anonymous transactions may be supported. Thus, the Intermediary **10** may serve as a form of proxy to blind transactions while providing security. In the case of medical records, for example, a complete authentication of the User **20** is performed, using any of a variety of means. For example, biometric methods, images, personal identification numbers (PINs) and passwords, alone or in combination with security tokens, such as the SecureID® card, may be employed. The particular level of authentication and the means employed are not a critical aspect of the invention, and therefore the most appropriate means may be selected. Indeed, the Intermediary **10** may support a plurality of authentication schemes, while it may deliver to the Data Repository **30** merely an indication of a successful authentication process.

The Intermediary **10** may impose a set of access rules, stored in the Rule Database **18**. These rules, for example, define which Users **20** may access which types of Records.

The Intermediary **10** does not normally hold encrypted information records for two reasons. First, this defeats the three-party security scheme and might compromise the security of the records themselves and second, this often means replicating and transporting potentially large databases. Rather, the Intermediary **10** provides transactional support for the Data Repository **30**, performing a number of tasks that are potentially burdensome. For example, in some instances, the User **20** will require exception processing. For example, in the case of a physician, normally a patient will specifically authorize transmission of a medical record, and therefore highly automated processing may be employed. In emergency situations, however, direct and complete confirmation of authorization may not be possible. In this case, often a manual authentication process will ensue. Likewise, in some cases, a User **20** will fail a biometric test or otherwise not have a required piece of information or security or Authentication Token **23**. Likewise, some Users **20** will be automated devices, which may employ special automated authentication protocols. A means is therefore provided for graceful recovery from these situations through exception processing, which may include manual intervention. Thus, this transactional burden may be shifted from the Data Repository **30** to the Intermediary **10**.

During an emergency request for authorization for example where a physician is properly authenticated as the User **20**, but the associated patient is unavailable for authentication or authentication is otherwise not possible, the system provides an emergency override mode of operation. In the case of record inputs to the system, the proffered record is assigned a default set of access privileges, and flagged as being an emergency (unauthenticated) record. Later, this record can be fully authenticated, and a specific set of access privileges assigned, when the patient is available, and the emergency flag removed.

When information is requested from the system in the absence of a complete patient authentication, the role of the physician is analyzed for consistency with the nature of the request. A restrictive set of access privileges may be applied, limiting access to only those records originally determined or coded to be "critical", which indeed may have both temporal and contextual sensitivity. Further, the nature of the emergency is analyzed, in addition to the role of the requester, to further restrict the information available. A personal communication may be initiated to allow a discretionary decision to be made. The accounted transaction fee may take into consideration the costs of authentication and verification; risks borne by the Intermediary or others; and the emergent nature of the requests. Thus, one embodiment of the present invention provides an insurance or indemnity accounting fee for consummating an information transaction.

The Intermediary **10** receives from the User **20** four (or more) pieces of information. As discussed above, the accounting and authentication information are provided. In addition, an identifier of the information sought (or to be transmitted) is also communicated. This is represented in FIG. **1** as the Transaction ID, and typically includes particulars of the record, e.g., patient identification in a medical record system, etc. The Intermediary **10** translates a portion of the Transaction ID into a Record ID, using a Record-Transaction Translation Table **17**. The Transaction ID may also include other particulars of the transaction. Finally, the User **20** maintains a public key encryption Key Pair Generator **22**. This Key Pair Generator **22** generates a Session Key pair, of which one component is maintained by the User **20** in secrecy, and the other component is transmitted. The User **20** also maintains a Secure Local Storage **21** system, for example for receipt of the private information and to store decryption information, such as the private portion of the key generated by the Key Pair Generator **22**.

In a medical environment, the Intermediary **10**, as part of the authentication, verifies that the User **20** has an appropriate set of rights to receive the requested information, for example, in a role-based authentication scheme. It is also possible for this "role" information to be passed to and processed by the Data Repository **30**, since an access privilege database need not be maintained by the Intermediary **10**, and the database might include sensitive information.

The Intermediary **10**, after authenticating the User **20**, and accounting and logging the transaction, processes the User **20** Public Session Key by internally multiplying this with an Intermediary Private Session Key, generated by the Key Pair Generator **16** and a Record Private Key maintained in a Secure Private Key Database **14**. The resulting value is then transmitted, along with the record identification, User **20** identification, and appropriate authentication and transactional logging data, to the Data Repository **30**.

In some instances, the User **20** authentication may include an associated identifier, for example a Patient-specific Public Key (ID Public Key) in a medical record system, which allows an additional or substitute layer of security. In

addition, a patient could himself act as a User **20**, seeking access to his or her own medical records.

In one scenario, the Data Repository **30** receives the information from the Intermediary **10**, and recalls the identified record from an Encrypted Database **31**. The database record remains encrypted with a Record Public Key, originally generated by the Key Pair Generator **16**. The Record Public and Private Keys, in this case, is stored in the Secure Record Key Database **14**. An Encryption Processor **15** may be provided to carry the cryptographic processing burden of the Intermediary **10**, for example implementing a secure socket layer (SSL) protocol. The encrypted database record from the Encrypted Record Database **31**, is presented to the Remote Key Handler **33**, a privileged processing environment having both high security and substantial cryptographic processing capacity. The Remote Key Handler **33** implements the algorithm:

$$C^{x}=C^{d_{record}\cdot d_{intermediary}\cdot e_{user}} \bmod n,$$

wherein:

d_{record} is the Record Private Key.

$d_{intermediary}$ is the Intermediary Private Session Key.

e_{user} is the User Public Session Key,

C is the ciphertext message stored in the Encrypted Record Database, encrypted with the e_{record}, the Record Public Key, and

C* is the ciphertext message in a composite-key transcrypted format for transmission to the User.

Likewise, for record accession into the Encrypted Record Database **31** from the User **20**, the Remote Key Handler **33** implements the algorithm:

$$C=C^{*e_{record}\cdot d_{intermediary}\cdot e_{user}} \bmod n,$$

wherein:

e_{record} is the Record Public Key,

$d_{intermediary}$ is the Intermediary Private Session Key,

e_{user} is the User Public Session Key,

C is the ciphertext message to be stored in the Encrypted Record Database, encrypted with the e_{record}, the Record Public Key, and

C* is the ciphertext message in a composite-key transcrypted format, received from the User.

It is noted that, while the public key generally corresponds to the encryption key (e), and the private key generally corresponds to the decryption key (d), in the present example, the Remote Key Handler **33** is considered privileged, and therefore receives a key containing the key component designated private. Since the encryption and decryption functions are complementary, the results are the same. The user therefore always applies its own private session key and the intermediary's public session key, regardless of the transaction type. This processing is performed in the Remote Key Handler **33**, based on information from the Intermediary **10** transmitted through a communications channel. This communications channel is preferably secure, such as a virtual private network. The Remote Key Handler **33** is preferably physically proximate or part of the Data Repository **30**.

The Data Repository **30** also receives a message intended for it from the Intermediary **10**, and may log the transaction using the supplied information. The Data Repository **30** further employs the User Identification to query a Certification Authority **40**, maintaining a Public Key Database **41**, in order to retrieve a persistent User Public Key. This User Public Key is then further employed by the Encryption Processor **32** to encrypt the Record for communication to the User **20**.

In another scenario, the User **20** transmits a Data Record to the Data Repository **30**. In this case, the Data Record is encrypted with the User **20** Private Session Key, the Intermediary **10** Public Session Key (received from the Intermediary during a handshaking communications), as well as the User **20** Persistent Private Key corresponding to the certificate stored by the Certification Authority **40** in the public key database **41**. The Data Repository **30** then receives the communication, first decrypts it with the User **20** Persistent Public Key received from the Certification Authority **40** from the Public Key Database **41** in the Encryption Processor **32**, and then passes it to the Remote Key Handler **33**, which securely receives a composite User Public Session Key. Intermediary Private Session Key Record Public Key product from the Intermediary **10**. This is employed by the Remote Key Handler **33** to produce a transcrypted Data Record, encrypted with the Record Public Key (generated by the Intermediary **10** in the Key Pair Generator **16**). This Record (encrypted with the Record Public Key) is then passed to the Data Repository **30** and stored in the Encrypted Database **31**.

It is noted that in anonymous communications, a proxy may be employed to blind the address of the User **20** from the Data Repository **30**. In this case, a modified scheme is employed which may not use a Certification Authority **40**, although the Intermediary **10** may provide anonymous certificate services.

It is also noted that each communication channel may itself be secure, for example using 128 bit secure socket layer (SSL) communications or other secure communications technologies. In particular, it is important that only the Intermediary **10** be in possession of the transcryption key (e.g., composite key) and the session key (e.g. Intermediary Private Session Key), since this will allow recovery of the private encryption key.

As noted above, the release of private keys may be limited by having both the Intermediary **10** and User **20** each generate a respective session key pair. In this case, the Intermediary **10** transmits the public portion of its session key pair to the User **20**, which is then employed to decrypt the message from the Data Repository **30**. The key provided by the Intermediary **10** to the Remote Key Handler **33**, in this case, is the product:

Record Private Key·User Public Session Key·Intermediary Private Session Key.

The resulting transcrypted record from the Data Repository **30** is encrypted with the product of the two session keys. Because the transmitted key is a triple composite, the Record Private Key is protected against factorization. The User **20** then uses the User Private Session Key and Intermediary Public Session Key in order to decrypt the Data Record.

In the case of a Data Record transmission from the User **20** to Data Repository **30**, the User **20** transmits a record encrypted with the product

User Private Session Key·Intermediary Public Session Key

Intermediary **10** transmits to the Remote Key Handler **33**, the product:

Public Record Key·User Public Session Key·Intermediary Private Session Key

which is used to transcrypt the encrypted Data Record with the Public Record Key.

In like manner, the Data Repository **30** may also generate a session key pair, used to sign and authenticate transmissions.

It is therefore seen that, by advantageously using the property of multiplicative identity of modulo arithmetic and the difficulty in factoring large semi-prime numbers, useful additions to the RSA encryption scheme are obtained. These additions allow secure third party involvement in communications, and the substitution of encryption keys without directly passing through a plaintext state.

Example 2

The transactional details of a second embodiment of the invention are now described with respect to FIG. **2**. FIG. **2** is similar to FIG. **1**, with a number of simplifications, and notably, an absence of a direct communications path between the User **120** and the Data Repository **130**. This allows an anonymous communication through the Intermediary **110** as a proxy.

As shown in FIG. **2**, the User **120** transmits a datastream to the Intermediary **110**, which includes authentication information, the User's public key, and a message encrypted with:

User Private Key·Private Session Key·Data Repository Public Key

The Intermediary **110** resorts to its Authentication Database **113**, PKI Certification Database **119** and Rule Database **118** to verify the authority and access privileges of the User **120**. The transactional details are stored in the Transaction Log **112**. During the initial communication between the User **120** and Intermediary **110**, the Intermediary **110** generates a Public and Private Session Key pair in the Key Pair Generator **116**, and transmits one portion to the User **120**.

The Intermediary **110** then transcrypts the message transmitted by the User **120** by performing an RSA type decryption operation on the message using the User **120** Public Key, effectively removing personally identifying information from the message while assuring the authenticity and authority of the User **120**. The anonymous message is then transmitted to the Data Repository **130**, which may then decrypt the message using the other portion of the Session Key (provided by the Intermediary **110**) and its own Private Key.

Example 3

FIG. **3** shows a simplified generic schematic arrangement for a three-party transaction. In FIG. **3**, three parties are involved in communication of a message. Separate authentication authorities, may serve as traditional certification authorities in a public key infrastructure, or may provide greater or lesser services to respective parties, or may be integrated within one or more of the three integral parties. FIG. **3** shows that the User **320** communicates message set-up information with the Intermediary **310**, in a communication In which the authenticity of the parties may be verified by Authentication Authority **341**. The Intermediary **310** correspondingly communicates message set-up information to Data Repository **330**, in a communication in which the authenticity of the parties may be verified by; Authentication Authority **342**. Finally, the Data Repository **330** and User **320** conduct an encrypted communication in either direction based on the set-up information, in a communication in which the authenticity of the parties may be verified by Authentication Authority **340**. If the Data Repository **330** initiates the communication, the flow paths are reversed. The Intermediary **310** is not a party to the communication proper, and has insufficient information to eavesdrop on the encrypted communication. In a generic case, a mere Diffie-Hellman type key exchange between the User **320** and Data Repository **330** would be sufficient; however, according to an aspect of the present invention, the Data Repository **330** and Intermediary **310** operate under mutual distrust to prevent release of a secret, which can only be transmitted for decryption to the User **320**. The Intermediary **310** holds the decryption key for the secret, while the Data Repository **330** holds the encrypted information. The communication set-up information therefore provides a scheme in which the Intermediary **310** passes a composite transcryption key to the Data Repository **330**, which includes as masked components the decryption key for the encrypted message, as well as a new session encryption key, for which the User **320** holds the corresponding session decryption key. Thus, neither the Intermediary **310** nor the Data Repository **330** ever possesses sufficient information to obtain message in decrypted form.

The Authentication Authorities **340**, **341**, **342** provide means for independent assurance that each party to the communication is the intended party, thus limiting the ability of any one party from undermining the security of the scheme. On the other hand, the ability of two parties to act together and in cooperation to obtain the secret message serves as a feature to allow recovery of the secret message in case of emergency.

Example 4

FIG. **4**A shows a work-flow diagram for the input of encrypted records by the User **20** with respect to the system of the Data Repository **30**. Initially, a Plaintext Record **401** is encrypted by the User **20** in a process **402** using the User Private Session Key **1***Intermediary Public Session Key **1**. The User **20** generates the User Private Session Key pair and receives the public portion of the Intermediary **10** Session Key communicated in the set-up communication. A message is then sent **403** from the User **20** to the Data Repository **30**, including the record encrypted with the composite (product of two or more PKI keys having the same modulus) session key **1** (User Private Session Key **1***Intermediary Public Session Key **1**). The Data Repository **30** passes **404** the encrypted record to the Remote Key Handler **40**. The Intermediary **10** then communicates **405** Composite Session Key **1** comprising the Intermediary Private Session Key **1***User Public Session Key **1*** Persistent Record Encryption Key. The Record encrypted with Composite Session Key **1** is then processed **406** in a transcryption process to yield a record encrypted with only the Persistent Record Encryption Key, the other key components having been eliminated. The record encrypted with the Persistent Record Encryption Key is then stored **407** in the Record Database **31** at the Data Repository **30**.

To output the record, as shown in FIG. **4**B, a complementary process is followed. A request is received **408** for the encrypted record. The Record encrypted with the Persistent Record Encryption Key is retrieved **409** from the Record Database **31** at the Data Repository **30**, and passed **410** to the Remote Key Handler **40**. The Intermediary **10** then transmits **411** to the Remote Key Handler **33** the Composite Session Key **2** comprising the Intermediary Private Session Key **2***User Public Session Key **2***Persistent Record Decryption Key. The Remote Key Handler **40** then processes **412** the Record encrypted with the Persistent Record Encryption Key with the received key to yield a Data

Record encrypted with the Composite Session Key **2** (Intermediary Private Session Key **2***User Public Session Key **2**), the Persistent Record Encryption Key having been eliminated in the transcryption process. The Record encrypted with Composite Session Key **2** is then passed **413** to the Data Repository **30**. The Data Repository **30** transmits **414** the encrypted Data Record encrypted with Composite Session Key **2** to the User **20**. The Data Record encrypted with Composite Session Key **2** is then decrypted **415** with the Intermediary Public Session Key **2***User Private Session Key **2**, the Intermediary Public Session Key **2** having been received from the Intermediary **10** and the User Private Session Key **2** being generated by the User **20** at the beginning of the transaction set-up. The User **20** thus obtains the plaintext record.

FIG. **5** provides a flowchart of the actions of the User **20** during typical transactions. The User **20** contacts **501** the Intermediary **10**, and during the ensuing communication the Intermediary **10** authenticates **502** the User **20**. After authentication **502**, the Intermediary **10** conducts **503** an optional accounting, implements rule and/or role based restrictions, and logs the transaction. The User **20** and Intermediary **10** then exchange **504** public session keys and optionally respective Persistent Public Keys, retaining their respective private session keys. A certification or Authentication Authority **541** may also provide further assurance of the identity of the various parties. The User **20** also defines **505** the nature of the desired transaction, for example uploading or downloading a Data Record. The intermediary **10** then communicates with a third party, e.g., the Data Repository **30**, in steps shown elsewhere.

An optional communication protocol is conducted **506** between the User **20** and a third party, e.g., the Data Repository **30**, to establish communication parameters and the like. In the case of a Data Record download, the User **20** receives **507** information from the third party encrypted with the User Public Session Key*Intermediary Private Session Key, and then decrypts **508** the information with the User Private Session Key*Intermediary Public Session Key. In the case of an upload of data, the User **20** sends **509** information to the third party encrypted with the User Private Session Key*Intermediary Public Session Key. The Certification Authority **540** may provide authentication services for communication between the User **20** and the third party.

FIG. **6** provides a flowchart of the actions of the Intermediary **10** during typical transactions. The User **20** contacts **601** the Intermediary **10**, and during the ensuing communication the Intermediary **10** authenticates **602** the User **20**. After authentication **602**, the Intermediary **10** conducts **603** an optional accounting, implements rule and/or role based restrictions, and logs the transaction. The User **20** and Intermediary **10** then exchange **604** public session keys, and optionally respective Persistent Public Keys, retaining their respective private session keys. A Certification Authority **641** or authentication authority may also provide further assurance of the identity of the various parties. The User **20** also defines **605** the nature of the desired transaction, for example uploading or downloading a Data Record. The Intermediary **10** then communicates **606** with a third party, e.g. the Data Repository **30**. This communication may be authenticated with Certification Authority **642** or authentication authority.

The Intermediary **10** then communicates **609** the Composite Session Key comprising the User Public Session Key*Intermediary Private Session Key*Persistent Record (Public or Private) Key to the third party, e.g. Data Repository **30** or Remote Key Handler **40**, depending on system architecture. The impending communication between third party and User **20** may be authenticated through the Certification Authority **640** or authentication authority.

FIG. **7** provides a flowchart of the actions of the third party, e.g., Data Repository **30** during typical transactions. The Intermediary **10** communicates **701** with the relevant third party or parties. The Intermediary **10** conducts **703** an optional accounting, implements rule and/or role based restrictions, and logs the transaction. The Intermediary **10** communicates **709** the Composite Session Key comprising the Intermediary Private Session Key*User Public Session Key*Persistent Record Encryption Key and optionally, the Persistent User Public Key, through the third party, to the Remote Key Handler **711**, where the Record Key is eliminated. A Certification Authority **742** may provide authentication services. The third party then sends **707** information to the User **20** encrypted with the User Public Session Key*Intermediary Private Session Key, or receives **710** from the User information encrypted with the User Private Session Key*Intermediary Public Session Key.

FIG. **8** provides a flowchart of the actions of the Remote Key Handler **40** during typical transactions. Communications are established **801** between the Remote Key Handler **40** and the Intermediary **10**. The Remote Key Handler **40** then receives **802** the Intermediary Private Session Key*User Public Session Key*Persistent Record Cryptographic Key (Public or Private). An encrypted file is received **803** through a Data Repository **30**, which is then transcrypted **804** with the received the Intermediary Private Session Key*User Public Session Key*Persistent Record Cryptographic Key (Public or Private). The transcrypted file is then transmitted **805** to the Data Repository **30**.

FIG. **9** provides a flowchart of an accounting protocol. Communications are established **901** between the User **20** and the Intermediary **10**. The User **20** is authenticated **902**. The transaction or proposed transaction is then accounted **903** for, for example by performing a financial charge against an account. The transaction and/or proposed transaction are then logged **904**. The transaction parameters are then tested for approval **905**, and if not approved, the transaction terminated **907** and various repercussions **908** implemented, for example, to ensure system security. If the transaction is approved, it is processed **906** and the Intermediary **10** communicates necessary key information, to facilitate the ultimate transaction between the User and the third party, e.g. Data Repository **30**.

Example 5

The algorithm according to the present invention may also be used in other circumstances where it is desired that a third party control decryption of a message without having access to the message itself. For example, a current trend is to secure electronic mail communications by providing a third party encryption, wherein the recipient must request a decryption key from a third party in order to reveal the message. This is advantageous, for example, where the availability of the decryption key is time limited, thus allowing the electronic communication to expire. According to the www.disappearing.com system, a symmetric cipher, i.e., the so-called Blowfish cipher, is employed. Therefore, if the encrypted message is made available to the server which hosts the encryption key, the privacy of the message is potentially impaired.

According to the present invention, see FIG. **3**, the Intermediary never has access to sufficient information to

decrypt any publicly transmitted information. Presuming that the Data Repository (receiver of the information) and the User (sender of the information), choose to maintain the secrecy of the message, the interception of the message by the Intermediary does not impair the security of the system. Likewise, because security of the system does not require the Intermediary to be shielded from the ciphertext message, the Intermediary can, in fact, serve as a proxy or host for the communications, see FIG. **2**.

Thus, in implementation, a secure three party communication system is provided as follows. The User **320** creates a message for the Data Repository **330**. The Data Repository **330** publishes a public key, which is available to the User **320**. The Intermediary **310** receives a message from the User **320**, initiating a transaction. The User **320** receives the Intermediary Public Session Key from the Intermediary **310** as well as a unique identifier for the message. The User **320** then computes the composite encryption key from Data Repository Public Key*Intermediary Public Session Key, and encrypts the message using this composite key, and sends it to the Data Repository **330**.

In order to decrypt the message, the Data Repository **330** communicates with the Intermediary **310**, provides the unique identifier of the message, and receives the Intermediary Private Session Key. The Data Repository **330** then computes the composite decryption key from Data Repository Private Key*Intermediary Private Session Key, and decrypts the message using this composite key.

The session key pair generated by the Intermediary **310** is used once, and may be expired or controlled based on a set of rules. Thus, the Intermediary **310** may have a policy of destroying keys after a set time period or upon existence of a condition. Since the security of the encryption is analogous to RSA-type encryption, it can be made relatively secure. Since the Intermediary **310** has no access to the Data Repository Private Key, the message cannot be decrypted based on information available to it. In addition, higher order composite keys may be implemented, for example composites formed of three or more RSA-type keys, some of which may be enduring keys (for example to provide digital signature capability) and other session keys.

It is noted that various features of the known Disappearing Inc. (San Francisco, Calif.) system, expressly incorporated herein by reference, may be employed in conjunction with the present invention. Thus, for example, special application software may be provided for restricting use by the recipient, thus preventing circumvention of the key restrictions.

Example 6

Another example according to the present invention provides a system for communicating a private message between two parties, wherein a third party controls access by the recipient to the message. Thus, an encrypted communication is sent by arbitrary means to a recipient, and a third party key management agent must communicate decryption information to the recipient in order to comprehend the message.

According to the present invention, in order for the recipient to obtain the necessary decryption information, accounting, authentication, and logging are implemented. According to a preferred embodiment, the decryption is preferably implemented by controlled application software, which prevents export of the message, such as by printing, disk storage, or the like. Therefore, within a reasonable extent, the message is isolated within the controlled application. The right of the user to access a comprehensible version of the message may be temporally limited, for example with an expiration date. These rights may also be limited based on a specified condition. Further use would require either a new transmission of the message, or a further accounting and logging of activity. Further, this allows control over the message on a per use basis, potentially requiring each user of the controlled application to authenticate himself or herself, and provide accounting information. Each use and/or user may then be logged.

It is also possible to permit anonymity of one party, for example a sender of a message, by employing anonymous cryptographic protocols, such as a employed in micropayment technology. Thus, a sender of a message may provide an anonymous accounting by employing an anonymous micropayment to account for the message transmission.

This technique therefore provides client-side security for messages, including medical records. By employing a third party for key management, burden on the sender is reduced.

Other embodiments will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. It is intended that the specification and examples be considered as exemplary only, with a true scope of the invention being indicated by the following claims.

APPENDIX

Prior Art References

A number of fields of endeavor are relevant to the present invention, and exemplary prior art, incorporated herein by reference, are disclosed below. The references disclosed provide a skilled artisan with embodiments of elements of the present invention, and the teachings therein may be combined and subcombined in various manners in accordance with the present teachings. The topical headings are advisory only, and are not intended to limit the applicability of any reference.

Medical Record Systems

John D. Halamka, Peter Szolovits, David Rind, and Charles Safran, "A WWW Implementation of National Recommendations for Protecting Electronic Health Information", J. Am. Med. Inform. Assoc. 1997 4: 458–464 (expressly incorporated herein by reference).

Reid Cushman, "Serious Technology Assessment for Health Care Information Technology" J. Am. Med. Inform. Assoc. 1997 4: 259–265 (expressly incorporated herein by reference).

Suzy A. Buckovich, Helga E. Rippen, and Michael J. Rozen, "Driving Toward Guiding Principles: A Goal for Privacy, Confidentiality, and Security of Health Information", J. Am. Med. Inform. Assoc. 1999 6: 122–133 (expressly incorporated herein by reference).

Paul C. Tang, "An AMIA Perspective on Proposed Regulation of Privacy of Health Information", J. Am. Med. Inform. Assoc. 2000 7: 205–207 (expressly incorporated herein by reference).

Clement J. McDonald, "The Barriers to Electronic Medical Record Systems and How to Overcome Them", J. Am. Med. Inform. Assoc. 1997 4: 213–221 (expressly incorporated herein by reference).

Suzy Buckovich, Helga Rippen and Michael Rozen, Driving Toward Guiding Principles: A Goal for Privacy, Confidentiality, and Security of Health Information, 6 Journal of the American Medical Informatics Association 122–133 (1999).

Helen Alderman and Caroline Kennedy, The Right to Privacy, pp. 140–143, 323–332.

James J. Cimino, Beyond the Cimino, Beyond the Superhighway, Exploiting the Internet with Medical Informatics, 4 Journal of the American Medical Informatics Association 279–284 (1997).

Paul Clayton, For the Record: Protecting Electronic Health Care Information 1997

Morris Collen, A Vision of Health Care and Informatics in 2008. 6 Journal of the American Medical Informatics Association 1–5 (1999).

Computer Science and Telecommunications Board, National Research Council, Networking Health: Prescriptions for the Internet (2000).

Reid Cushman, Serious Technology Assessment for Health Care Information Technology, 4 Journal of the American Medical Informatics Association 259–65 (1997).

Department of Health and Human Services, Standards for Privacy of Individually Identifiable Health Information; Final Rule, 56 Federal Register 82462–82829.

Robert E. DeWitt, Anita Ellis, Harton, William E. Hoffmann, Jr., Robert M. Keenan, III, and Marie B. Russell, Patient Information and Confidentiality in Treatise on Health Care Law (eds., 1998).

The Drummond Group, The HealthKey Program: PKI in Healthcare.

Aviva Halpert, Access Audit Trails: En Route to Security, Journal of AHIMA (September 2000).

Health Privacy Project, Summary of New Federal Health Privacy Regulations at http://www.healthprivacy.org.

Isaac Kohane, F. J. van Wingerde, James C. Fackler, Christopher Cimino, Peter Kilbridge, Shawn Murphy, Henry Chueh, David Rind, Charles Safran, Octo Barnett, and Peter Szolovits, Sharing Electronic Medical Records Across Multiple Heterogeneous and Competing Institutions.

New York State, Public Health Law, Article 29 (Health Care Agents and Proxies).

D. M. Rind, L S. Kohane, P. Szolovits, C. Safran, H. C. Chueh, and G. O. Barnett, Maintaining the confidentiality of medical records shared over the Internet and the World Wide Web, Annals of Internal Medicine 1997: 127: 138–141.

Thomas C. Rindfleisch, Privacy, Information Technology and Healthcare, Communications of the ACM, Vol. 40, No. 8, August 1997.

John Roberts, Sheila Decter, and Denise Nagel, Letter to the Editor [regarding Confidentiality and Electronic Medical Records], Annals of Internal Medicine, 15 Mar. 1998.

Charles Safran et al. Protection of Confidentiality in Computer Based Patient Records, MD Computing, Vol. 12, No. 3, May 1995.

Edward H. Shortliffe, The Next Generation Internet and Healthcare: A Civics Lesson for the Informatics Community, at www.amia.org/pubs/symposia/D005232.pdf.

Peter Szolovits, A Revolution in Electronic Medical Records Systems via the World Wide Web at http://www.emrs.org/publications/IAHIT.html.

Peter Szolovits, Jon Doyle, William J. Long. Isaac Kohane, and Stephen G. Pauker, Guardian Anabel: Patient Centered Health Information Systems at http://www.ga.org/ga/manifesto/GAtr.html.

Peter Szolovits, Cryptography Based Patient Identifier at http://nevhs.hhs.gov/app7-**4**.htm.

U.S. Congress, Office of Technology Assessment, Protecting Privacy in Computerized Medical Information, OTA-TCT-576 (September 1993).

L. L. Weed, Medical Records, Medical Education, and the Patient: The Problem Oriented Medical Record as a Basic Tool, Case Western University Press, 1971.

U.S. Pat. No. 5,361,202 (Doue, Nov. 1, 1994, Computer display system and method for facilitating access to patient data records in a medical information system), expressly incorporated herein by reference, relates to a system and method to improve access to patient information in medical information system for a health care facility. A computer display system, and a method for such a display system, includes a displayed representation of the duration of the stay of an identified patient in the health care facility. In such a medical information system patient data is stored in data files in a database, wherein each data file in the database is comprised of a plurality of data records. A User positions a cursor on the displayed representation using an input unit and signals the computer of a desired date and time. The computer, in response to the signal determines the desired date and time from the position of the cursor and accesses a data record or records from the data file based on the desired date and time. The accessed data record or records may then be displayed. The data records may be time-stamped. In that case, the duration of the patient's stay is the time period between the earliest and latest time stamps.

U.S. Pat. No. 5,644,778 (Burks, et al., Jul. 1, 1997, Medical transaction system), expressly incorporated herein by reference, relates to a medical transaction system, which is capable of permitting a plurality of healthcare providers to communicate with a plurality of payors and financial institutions. The healthcare providers, payors, and financial institutions do not have to communicate in the same data message formats nor in the same communication protocols. Such a system facilitates not only the processing of medical claims submitted by the healthcare providers to the payors, but also permits the transfer of medical data records between healthcare providers. The system supports the processing of medical claims without requiring a centralized database or imposing a uniform claim format on the healthcare providers and payors. The preferred embodiment further includes a financial transactor that uses remittance information from the payors to generate the electronics funds transfer messages to credit and debit accounts. Additionally, the system supports a medical line of credit at financial institutions that may be used to pay portions of medical claims not covered by payors.

U.S. Pat. No. 5,832,450 (Myers, et al. Nov. 3, 1998), expressly incorporated herein by reference, provides an electronic medical record system that stores data about individual patient encounters arising from a content generator in free-form text. A header for each encounter-based record also uses text to store context information for that record. Each header comprises a plurality of attributes embodied as a field descriptor and a value, bound together as a text object. By binding the field descriptors to the values, each encounter record is complete in itself, without reference to database keys, thereby providing a self-validating record storage system. In this system, the security of the medical data is maintained, because the attribute values and the attribute descriptors are bound together as a text object, and because the values are not location dependent, the data is self-validating. Thus, templates, keys, or other lookup means employed by relational database are not required to find or interpret the data. Additional attributes may be added without a restructuring process, reducing a source of errors into the system. Access of the content and context information in the EMR system by external systems is possible without secondary tables or keys.

U.S. Pat. No. 5,546,580 (Seliger, et al., Aug. 13, 1996), expressly incorporated herein by reference, relates to a method and apparatus for coordinating concurrent updates to a medical information database, from different workstations and medical instruments. A first data value for a record is entered at a first workstation and a second data value for the record is entered at a second workstation without locking either workstation during data entry. The new data values are stored in the medical database after completion of data entry at each workstation, and a correction history is recorded. The correction history contains information as to the update of the record with the first data value and the second data value. The record is updated with the first and second data values without aborting user activities or notifying a user that an update conflict has occurred. After the new data values are stored in the medical database, all workstations containing a copy of the record are updated to reflect the current state of the record.

U.S. Pat. No. 5,832,488 (Eberhardt, Nov. 3, 1998), expressly incorporated herein by reference, relates to a computer system and method for storing medical histories using a smartcard to store data. A computer system and method is provided for programming it for storage of individual medical histories on a storage device, preferably about the size of a credit card, for adding new medical data about the individual to the device and for communicating with other computers to retrieve large data records about the individual; and for enabling a second computer to collate and sort data relating to selected medical fields from the data of such individual and from the data about other individuals transferred to the second computer.

U.S. Pat. No. 5,867,821 (Ballantyne, et al., Feb. 2, 1999), expressly incorporated herein by reference, relates to a method and apparatus for electronically accessing and distributing personal health care information and services in hospitals and homes, for the distribution and administration of medical services, entertainment services, electronic medical records, educational information, etc. to a patient's individual electronic patient care station (PCS) interconnected to a master library (ML) which stores data in digital compressed format, through a local medical information network. The patient/medical personnel interact with this medical information network through the unique PCS and receive the requested service or data from the master library. The data is then displayed either on the associated television set or video monitor or through wireless/IR communications to a peripheral personal data assistant (pen based computer technology) The data for text, audio, and video information is all compressed digitally to facilitate distribution and only decompressed at the final stage before viewing/interaction.

U.S. Pat. No. 5,899,998 (McGauley, et al., May 4, 1999), expressly incorporated herein by reference, relates to a method and system for maintaining and updating computerized medical records. A distributed database architecture stores medical information in a self-updating system that employs point-of-service stations disposed at convenient medical service locations. Each patient carries a portable data carrier such as a smart card that contains the patient's complete medical history. Interaction between the portable data carriers and the point-of-service stations effects a virtual communication link that ties the distributed databases together without the need for online or live data connections. The point-of-service stations are also interconnected over a communications network through a switching station that likewise does not rely on online, live communication. The database system uses an object-oriented update object to distribute data that has been generated when a portable data carrier is not physically present and to automatically distribute data without the necessity of accessing a masterfile.

U.S. Pat. No. 5,903,889 (de la Huerga, et al., May 11, 1999), expressly incorporated herein by reference, relates to a system and method for translating, collecting and archiving patient records. The system retrieves, modifies, and collects data records having a plurality of formats and distributed on a plurality of databases on a computer network. The system includes means for detecting various types, relationships, and classifications of data records and modifying them accordingly to support interactive, hypertext-linked display of, and organized access to, the data records. The system further includes means to store a related set of data records on a mass storage device such as a CD-ROM to provide non-network access to the data records. Adapted for use in a hospital environment, the system facilitates access by care providers, administrators, and insurance company agents to a patient's cumulative, and possibly extensive, record.

U.S. Pat. No. 5,911,132 (Sloane, Jun. 8, 1999, Method using central epidemiological database), expressly incorporated herein by reference, relates to a system in which patient disease is diagnosed and/or treated using electronic data communications between not only the physician and his/her patient, but via the use of electronic data communications between the physician and one or more entities which can contribute to the patient's diagnosis and/or treatment, such electronic data communications including information that was previously received electronically from the patient and/or was developed as a consequence of an electronic messaging interaction that occurred between the patient and the physician. Such other entities illustratively include a medical diagnostic center and an epidemiological database computer facility that collects epidemiological transaction records from physicians, hospitals and other institutions that have medical facilities, such as schools and large businesses. The epidemiological transaction record illustratively includes various medical, personal and epidemiological data relevant to the patient and his/her present symptoms, including test results, as well as the diagnosis, if one has already been arrived at by the e-doc. The epidemiological database computer facility can correlate this information with the other epidemiological transaction records that it receives over time in order to help physicians make and/or confirm diagnoses as well as to identify and track epidemiological events and/or trends.

U.S. Pat. No. 5,911,687 (Sato, et al., Jun. 15, 1999, Wide area medical information system and method using thereof), expressly incorporated herein by reference, relates to a wide area medical information system and a method using thereof comprising a wide area network, a plurality of doctor terminals and patient terminals connected to the wide area network, and a management server including at least an electronic case record file storing clinic information for patient's and a doctor database storing data of a plurality of doctors, wherein the system searches the doctor database on the basis of patient information including the condition of the disease of a certain patient input from the patient terminal, selects the corresponding doctor, requests that the selected doctor take charge of examination and treatment for the aforementioned certain patient, registers the correspondence between the approved doctor and the aforementioned certain patient in the electronic case record file, gives the right to access the clinic information of the patient to the approved doctor, and executes the online examination and treatment via the doctor terminal and patient terminal, so that a patient existing in a wide area can receive remote

examination and treatment services of high satisfaction and medical treatment related services other than examination and treatment without depending on the location.

U.S. Pat. No. 5,915,240 (Karpf, Jun. 22, 1999), expressly incorporated herein by reference, relates to a computer system and method for accessing medical information over a network. The system partitions the functioning of the system between a client and server program optimized in a manner to assure synchronization of the master medical information databases on the servers with the local medical information database on the client, minimize the use of network resources, and allow new types of medical information to be easily included in the system. A server site on the network maintains a description of its medical information, as well as the most current and up-to-date medical reference information. The client program maintains a local database that is automatically synchronized over the network with revisions and new medical information, and provides a user with an interface to fully review the information in the database. The system also uses a context-sensitive call facility so that users of the Medical Lookup Reference program can easily get further expert assistance about the medical topic. The call feature uses the network connection to establish a conversation between the user and a person at a help site specified by the type of medical information they are currently referencing. Once a connection is established, the system allows the user to engage in a conversation with the person at the help site, and a record of the conversation can be saved in a database for auditing purposes.

U.S. Pat. No. 5,924,074 (Evans, Jul. 13, 1999), expressly incorporated herein by reference, relates to an electronic medical records system. The system captures patient data, such as patient complaints, lab orders, medications, diagnoses, and procedures, at its source at the time of entry using a graphical user interface having touch screens. Using pen-based portable computers with wireless connections to a computer network, authorized healthcare providers can access, analyze, update and electronically annotate patient data even while other providers are using the same patient record. The system likewise permits instant, sophisticated analysis of patient data to identify relationships among the data considered. Moreover, the system includes the capability to access reference databases for consultation regarding allergies, medication interactions and practice guidelines. The system also includes the capability to incorporate legacy data, such as paper files and mainframe data, for a patient.

U.S. Pat. No. 5,933,809 (Hunt, et al., Aug. 3, 1999), expressly incorporated rein by reference, relates to computer software for processing medical billing record information. Hospital or individual doctor Medicare billing records are processed using computer software. The software contains at least one set of instructions for receiving, converting, sorting and storing input information from the pre-existing medical billing records into a form suitable for processing. The software contains at least one set of instructions for processing the input medical billing record information, preferably to identify potential Medicare "72 hour billing rule" violations. This processing is preferably performed by comparing each input medical billing record containing dates of medical inpatient admission and discharge to each input medical billing record containing a date of medical outpatient service. The inpatient and outpatient billing records are first compared to determine if they contain matching patient identification codes to identify all the records originating from the same patient. If matching patient identification codes are found the inpatient and outpatient billing records are further compared to determine if the date of outpatient service fell within a preselected time period, preferably 72 hours, prior to the date of inpatient admission. If so, the matching inpatient and outpatient billing records are distinguished and stored separately for further processing. If not, the matching inpatient and outpatient billing records are compared to determine if the date of outpatient service fell between the inpatient admission and discharge dates. If this is the case, the matching inpatient and outpatient billing records are again distinguished and stored separately for further processing. If not, the program proceeds to the next set of billing records to repeat the sequence.

U.S. Pat. No. 5,974,389 (Clark, et al., Oct. 26, 1999, Medical record management system and process with improved workflow features) relates to a patient medical record system includes a number of caregiver computers, and a patient record database with patient data coupled to the caregiver computers selectively providing access to the patient data from one of the caregiver computers responsive to a predetermined set of access rules. The predetermined set of rules includes a rule that access to a predetermined portion of the patient data by a first caregiver must be terminated before access to the same predetermined portion by a second caregiver is allowed.

U.S. Pat. No. 5,991,758 (Ellard, Nov. 23, 1999), expressly incorporated herein by reference, relates to a system and method for indexing information about entities from different information sources. A system and method for indexing a data record from an information source into a database, the database containing a plurality of data records, is provided comprising receiving a data record from an information source, the received data record having a predetermined number of fields containing information about a particular entity, standardizing and validating the data in the received data record. A system and method is also provided for retrieving records that refer to an entity characterized by a specific set of data values by comparing a predetermined number of fields within the received data record with a predetermined number of fields within the data records already in the database, selecting data records already in the database as candidates having data within some of the predetermined fields that is identical to the data in the fields of the received data record, and scoring the candidates to determine data records having information about the same entity.

U.S. Pat. No. 5,995,943 (Bull, et al., Nov. 30, 1999), expressly incorporated herein by reference, relates to an information aggregation and synthesis system. An information aggregation and synthesis system and process, which provides aggregation and packaging of structured or unstructured information from disparate sources such as those available on a network such as the Internet. A user operates a network compatible/addressable interface device. The network interface device communicates with local datastores or network accessible datastores via an addressing scheme such as Uniform Resource Locator addresses (URLs) utilized by the Internet. Data passing between the network interface device and the datastores is accessed, polled, and retrieved through an intermediary gateway system. Such aggregated information is then synthesized, customized, personalized and localized to meet the information resource requests specified by the user via the network interface device.

U.S. Pat. No. 6,012,035 (Freeman, Jr., et al., Jan. 4, 2000), expressly incorporated herein by reference, relates to a system and method for supporting delivery of health care.

Effectuation of a health care provision agency cooperative function is established through a communication network linking all the various entities of the cooperative. The entities include the third party payor members, the health providing individuals, clinics, or the like, along with secondary providers including pharmacies and laboratories, health care facilities such as hospitals, and the several entities associated with management of the cooperative and appropriate funds transfer functions. A coordinating interface system maintains data storage of the necessary information, and manages the entity intercommunications in accordance with the basic structure of the active and eligible elements of the agency cooperative.

U.S. Pat. No. 6,035,276 (Newman, et al., Mar. 7, 2000), expressly incorporated herein by reference, relates to a system and method for selectively generating provider application forms required to be submitted to health care provider organizations by physicians and related health care professionals. Physician credentialing profiles containing physician credentialing information are stored into a system database together with a plurality of different provider application formats associated with particular application forms which are completed and selected data extracted from the common information contained in the stored physician credentialing profiles. The method automatically inputs a subset of physician credentialing information required by a particular selected provider application format into the provider application form associated with that format and generates the particular provider application form.

U.S. Pat. No. 6,055,494 (Friedman, Apr. 25, 2000), expressly incorporated herein by reference, relates to a system and method for medical language extraction and encoding. In computerized processing of natural-language medical/clinical data including phrase parsing and regularizing, parameters are referred to whose value can be specified by the user. Thus, a computerized system can be provided with versatility, for the processing of data originating in diverse domains, for example. Further to a parser and a regularizer, the system includes a preprocessor, output filters, and an encoding mechanism.

U.S. Pat. No. 6,055,506 (Frasca, Jr. Apr. 25, 2000) expressly incorporated herein by reference, relates to an outpatient care data system dedicated to the transmission, storage and retrieval of outpatient data relating to care of outpatients is provided with a regional data system located at a regional location, a plurality of metropolitan area data systems operatively connected to the regional data system, each of the metropolitan area data systems being located at a different metropolitan location. Each metropolitan area data system may be provided with an electronic nursing station located within a hospital and first and second types of outpatient systems operatively coupled to the electronic nursing station on a real-time basis. The first type of outpatient system is situated at a first non-hospital location remote from the hospital and includes a medical device associated with an outpatient present at the first non-hospital location, and the second type of outpatient system is situated at a second non-hospital location remote from the hospital and includes a medical device associated with an outpatient present at the second non-hospital location.

U.S. Pat. No. 6,076,066 (DiRienzo, et al., Jun. 13, 2000), expressly incorporated herein by reference, relates to an attachment integrated claims (AIC) system formed by a combination of first, second and third storage media. The first storage medium stores computer readable instructions for permitting a first computer system to receive textual data as field data, where each of the field data is displayed on a predetermined portion of a first screen of the first computer system, to assemble the field data and a corresponding digitized image into a first file having an integrated file format and to transmit the first file to a second computer system via a communications channel. The second storage medium stores computer readable instructions permitting the second computer system to receive the first file via the communications channel, to display the corresponding digitized attachment on a second screen of the second computer system, and to transfer the field data to a third computer operatively connected to the second computer. In addition, the third storage medium stores computer readable instructions permitting the third computer system to receive the field data from the second computer, to display the field data on a third screen and to generate a second file including portions of the field data extracted from the first file. In other words, the AIC system permits transmission of a customizable claim form and integrated attachment to an insurance carrier via a non-clearinghouse communications channel. An AIC system including several computers connected via a communications channel, an electronic file, and an operating method therefore are also described. In an exemplary case, the first file follows a predetermined graphic image interchange file format and the field data is incorporated into comment blocks associated with the predetermined graphic image interchange file format.

U.S. Pat. No. 6,076,166 (Moshfeghi, et al., Jun. 13, 2000), expressly incorporated herein by reference, relates to a system and method for personalizing hospital intranet web sites. The server includes a layer for dynamically generating web pages and other data objects using scripts, such as graphic, audio and video files, in dependence on stored information indicating the user's needs and preferences, including those presumed from stored information as to the user's function, job, or purpose for being at the hospital, and logged usage profiles, the level of the user's access privileges to confidential patient information, and the computer and physical environments of the user. Notably, the content is generated in dependence on the display resolution and lowest bandwidth link between the server and browser to limit the waiting time for downloads as well as the server load.

See also, U.S. Pat. No. 5,319,543 (Wilhelm, Jun. 7, 1994, Workflow server for medical records imaging and tracking system); U.S. Pat. No. 5,465,082 (Chaco, Nov. 7, 1995, Apparatus for automating routine communication in a facility); U.S. Pat. No. 5,508,912 (Schneiderman, Apr. 16, 1996, Clinical database of classified out-patients for tracking primary care outcome); U.S. Pat. No. 5,546,580 (Seliger, et al., Aug. 13, 1996, Method and apparatus for coordinating concurrent updates to a medical information database); U.S. Pat. No. 5,592,945 (Fiedler, Jan. 14, 1997, Real-time event charting in an electronic flowsheet); U.S. Pat. No. 5,619,991 (Sloane, Apr. 15, 1997, Delivery of medical services using electronic data communications); U.S. Pat. No. 5,664,109 (Johnson, et al., Sep. 2, 1997, Method for extracting predefined data items from medical service records generated by health care providers); U.S. Pat. No. 5,772,585 (Lavin, et al., Jun. 30, 1998, System and method for managing patient medical records); U.S. Pat. No. 5,778,882 (Raymond, et al., Jul. 14, 1998, Health monitoring system); U.S. Pat. No. 5,845,253 (Rensimer, et al., Dec. 1, 1998, System and method for recording patient-history data about on-going physician care procedures); U.S. Pat. No. 6,082,776 (Feinberg, Storing Personal Medical Information); U.S. Pat. No. 6,157,914 (Seto, Medical support system); U.S. Pat. No. 6,149,440 (Clark, Methods and apparatus for authenticating

informed consent); U.S. Pat. No. 5,779,634 (Ema, Medical information processing system for supporting diagnosis); U.S. Pat. No. 5,586,262 (Komatsu, Image data management system particulary for use in a hospital); U.S. Pat. No. 5,528,492 (Fukushima, Method of managing medical diagnosis data with reference relationship); U.S. Pat. No. 5,781,890 (Nematbakhsh, Method for managing clustered medical data and medical data filing system in clustered form), each of which is expressly incorporated herein by reference.

Rights-Based Access to Database Records

U.S. Pat. No. 6,192,476, expressly incorporated herein by reference, relates to a method for providing security, comprising the steps of detecting when a request for an action is made by a principal, and determining whether the action is authorized based on permissions associated with a plurality of routines in a calling hierarchy associated with the principal, wherein the permissions are associated with the plurality of routines based on a first association between protection domains and permissions.

U.S. Pat. No. 5,325,294 (Keene, Jun. 28, 1994), expressly incorporated herein by reference, relates to a medical privacy system. A method and apparatus for authorized access to medical information concerning an individual while preserving the confidentiality of, and preventing unauthorized access to, such information, is provided. A computer database receives and stores the individual's medical information, after the individual is tested to establish this information and the date on which such information was most recently obtained. The computer database does not contain the individual's name, address or any other similar information by which the individual can be identified. The individual is given an identification card containing a photograph or holographic image of the individual and containing a confidential first identification number that is unique for the individual, where both the image and the first identification number are visually perceptible and cannot be altered on the card without detection of such alteration. The individual is also given a confidential second identification number that is not contained on the card and need not be unique for that individual. The computer database can be accessed telephonically, and the individual's medical information, or a portion thereof, can be read only by an inquiror, if the inquiror or the individual first provides the individual's first and second identification numbers. The inquiror can use the image and first identification number on the individual's card to confirm the identity of that individual but need not be told the individual's second identification number. After inquiror establishes the identity of the individual, the inquiror, with the assistance of the individual, can obtain a telephonic readout of the individual's medical information.

U.S. Pat. No. 5,499,293 (Behram, et al., Mar. 12, 1996), expressly incorporated herein by reference, relates to a privacy protected information medium using a data compression method, which uses an efficient data compression/decompression scheme using a passive data storage media such as a card-based approach for storage of medical data information. The system operates on existing personal computer hardware in a medical center or doctors' offices, doing away with expensive investments in specialized technologies of central processing hardware. With the advent of inexpensive desktop computing, a number of inventions have been offered to improve medical information storage and retrieval. They include the development of portable medical card technologies such as SmartCards and optical cards, which are capable of storing medical information, and can be carried by the patient. This card-based system provides a methodology for storage and retrieval of medical information from a passive credit-card sized instrument. The card is manufactured with minimal expense using existing well-known optical scanning or magnetic tape reading or a data interrogation means in a SmartCard based system.

U.S. Pat. No. 5,987,440 (O'Neil, et al., Nov. 16, 1999), expressly incorporated herein by reference, relates to a personal information security and exchange tool. Utilization of the E-Metro Community and Personal Information Agents assure an effective and comprehensive agent-rule based command and control of informational assets in a networked computer environment. The concerns of informational privacy and informational self-determination are addressed squarely by affording persons and entities a trusted means to author, secure, search, process, and exchange personal and/or confidential information in a networked computer environment. The formation of trusted electronic communities wherein members command and control their digital persona, exchanging or brokering for value the trusted utility of their informational assets is made possible. The system provides for the trusted utilization of personal data in electronic markets, providing both communities and individuals aggregate and individual rule-based control of the processing of their personal data.

U.S. Pat. No. 6,029,160 (Cabrera, et al., Feb. 22, 2000), expressly incorporated herein by reference, relates to a system and method for linking a database system with a system for filing data. Extensions to a database system provide linkage between data in the database system and files in a system for filing data that is external to the database system ("the filing system"). The linkage includes an external file reference (efr) data type, which is defined in the database system for reference to files that are stored in the filing system. When entries are made in the database system that include efr data-type references to files in the filing system, control information is provided by the database system to the filing system. The control information causes the filing system to control processing of referenced files according to referential constraints established in the database system.

U.S. Pat. No. 6,038,563 (Bapat, et al., Mar. 14, 2000), expressly incorporated herein by reference, relates to a system and method for restricting database access to managed object information using a permissions table that specifies access rights corresponding to user access rights to the managed objects. An access control database has access control objects that collectively store information that specifies access rights by users to specified sets of the managed objects. The specified access rights include access rights to obtain management information from the network. An access control server provides users access to the managed objects in accordance with the access rights specified by the access control database. An information transfer mechanism sends management information from the network to a database management system (DBMS) for storage in a set of database tables. Each database table stores management information for a corresponding class of managed objects. An access control procedure limits access to the management information stored in the database tables using at least one permissions table. A permissions table defines a subset of rows in the database tables that are accessible to at least one of the users. The set of database table rows that are accessible corresponds to the managed object access rights specified by the access control database. A user access request to access management information in the database is intercepted, and the access control procedure is invoked when the user access request is a select statement. The database access engine accesses information in the set of

database tables using the permissions tables such that each user is allowed access only to management information in the set of database tables that the user would be allowed by the access control database to access.

U.S. Pat. No. 6,041,411 (Wyatt, Mar. 21, 2000), expressly incorporated herein by reference, relates to a method for defining and verifying user access rights to computer information. A method is provided for minimizing the potential for unauthorized use of digital information, particularly software programs, digital content and other computer information, by verifying user access rights to electronically transmitted digital information. A second computer system transmits requested digital information to a requesting first computing system in wrapped form, which includes digital instructions that must be successfully executed, or unwrapped, before access to the digital information is allowed. Successful unwrapping requires that certain conditions must be verified in accordance with the digital instructions, thereby allowing access to the digital information. In one embodiment, verification includes locking the digital information to the requesting computer system by comparing a generated digital fingerprint associated with the digital information to a digital fingerprint previously generated which is unique to the requesting computer system.

U.S. Pat. No. 6,044,401 (Harvey, Mar. 28, 2000), expressly incorporated herein by reference, relates to a network sniffer for monitoring and reporting network information that is not privileged beyond a user's privilege level. Nodes in the network include a network sniffer and an access sniffer. The access sniffer includes an access element and an access interface. The access element preferably includes a memory and a database. The access element accesses the network sniffer and filters out unavailable information by using information such as address and port numbers gathered by the network sniffer. Unavailable information includes information which is non-public or beyond the privilege level of the particular user. The access element evaluates data streams that are public information to determine if the data streams meet a predetermined criterion. If the data streams meet the predetermined criteria, then the data is saved in the database. The access element transfers only the information available to the particular user to the access interface. The access element can time itself for a limited amount of time for execution. Once the predetermined time period has expired, the access element is complete and it can save and transfer the appropriate information to the access interface.

U.S. Pat. No. 6,052,688 (Thorsen, Apr. 18, 2000), expressly incorporated herein by reference, relates to a computer-implemented control of access to atomic data items. The method comprises the steps of initiating and maintaining data access nodes in a variable access structure. Each access node is provided with references to other access nodes and/or to data items representing an object, each data item carrying only the amount of information that is relevant for its purpose. The data items or the references are provided with a time parameter thus enabling version control and the possibility to handle static or slowly changing data and frequently chanced and updated data in a corresponding manner. The access nodes comprise access control parameters for access control from a safety point of view as well as for enabling different views of the access structure and underlying data and objects.

U.S. Pat. No. 6,073,106 (Rozen, et al., Jun. 6, 2000), expressly incorporated herein by reference, relates to a method of managing and controlling access to personal information. A participant is prompted to provide a constant identifier and a selected password via Internet communications or via phone/fax/mail. Emergency and confidential categories of medical information are identified, and the participant is prompted to provide personal information in each of the categories and a different personal identification number (E-PIN, C-PIN) for each category. The participant is also prompted to provide an instruction to disclose or to not disclose the personal information in the emergency category in the event a requester of the information is an emergency medical facility and is unable to provide the participant's E-PIN. Alteration of any of the participant's medical information is enabled upon presentation of the participant's identifier and password by the requester. The emergency information or the confidential information is disclosed upon presentation of the participant's identifier and E-PIN or C-PIN. In addition, the emergency information is disclosed to an emergency medical facility verified as such by a service provider in the event the participant has provided an instruction to disclose the emergency information. Storage and access to health related documents such as healthcare power of attorney, consent for treatment, and eyeglass prescription is also provided.

U.S. Pat. No. 6,073,234 (Kigo, et al., Jun. 6, 2000), expressly incorporated herein by reference, relates to a device and method for authenticating user's access rights to resources. Both of a user side and a protect side such as a programmer of an application programmer need not handle a large number of inherent information such as authentication keys. An access ticket generation device generates an access ticket from user unique identifying information and access rights authentication feature information. As unique security characteristic information, there is used a secret key of an elliptic curve encryption or an ElGamal encryption. A proof data generation device receives the access ticket, converts authentication data received from a proof data verification device into proof data by use of the access ticket and the user unique identifying information, and returns the resultant proof data to the proof data verification device. The proof data generation device or the proof data verification device decrypts the above-mentioned encryption. The proof data verification device verifies the access rights as correct only when a combination of an access ticket and user unique identifying information used in the proof data generation device is correct.

U.S. Pat. No. 6,138,119 (Hall, Techniques for defining, using and manipulating rights management data structures), expressly incorporated herein by reference.

Role-Based Access

U.S. Pat. No. 6,023,765 (Kuhn, Feb. 8, 2000; Implementation of role-based access control in multi-level secure systems), expressly incorporated herein by reference, relates to a system and method for implementation of role-based access control in multi-level secure systems. Role-based access control (RBAC) is implemented on a multi-level secure (MLS) system by establishing a relationship between privileges within the RBAC system and pairs of levels and compartments within the MLS system. The advantages provided by RBAC, that is, reducing the overall number of connections that must be maintained, and, for example, greatly simplifying the process required in response to a change of job status of individuals within an organization, are then realized without loss of the security provided by MLS. A trusted interface function is developed to ensure that the RBAC rules permitting individual's access to objects are followed rigorously, and provides a proper mapping of the roles to corresponding pairs of levels and compartments. No other modifications are necessary. Access requests from

subjects are mapped by the interface function to pairs of levels and compartments, after which access is controlled entirely by the rules of the MLS system.

See also, U.S. Pat. No. 6,073,242 (Electronic authority server); U.S. Pat. No. 6,073,240 (Method and apparatus for realizing computer security); U.S. Pat. No. 6,064,977 (Web server with integrated scheduling and calendaring); U.S. Pat. No. 6,055,637 (System and method for accessing enterprise-wide resources by presenting to the resource a temporary credential); U.S. Pat. No. 6,044,466 (Flexible and dynamic derivation of permissions); U.S. Pat. No. 6,041,349 (System management/network correspondence display method and system therefore); U.S. Pat. No. 6,014,666 (Declarative and programmatic access control of component-based server applications using roles); U.S. Pat. No. 5,991,877 (Object-oriented trusted application framework); U.S. Pat. No. 5,978,475 (Event auditing system); U.S. Pat. No. 5,949,866 (Communications system for establishing a communication channel on the basis of a functional role or task); U.S. Pat. No. 5,925,126 (Method for security shield implementation in computer system's software); U.S. Pat. No. 5,911,143 (Method and system for advanced role-based access control in distributed and centralized computer systems); U.S. Pat. No. 5,797,128 (System and method for implementing a hierarchical policy for computer system administration); U.S. Pat. No. 5,761,288 (Service context sensitive features and applications); U.S. Pat. No. 5,751,909 (Database system with methods for controlling object interaction by establishing database contracts between objects); U.S. Pat. No. 5,748,890 (method and system for authenticating and auditing access by a user to non-natively secured applications); U.S. Pat. No. 5,621,889 (Facility for detecting intruders and suspect callers in a computer installation and a security system including such a facility); U.S. Pat. No. 5,535,383 (Database system with methods for controlling object interaction by establishing database contracts between objects); U.S. Pat. No. 5,528,516 (Apparatus and method for event correlation and problem reporting); U.S. Pat. No. 5,481,613 (Computer network cryptographic key distribution system); U.S. Pat. No. 5,347,578 (Computer system security); U.S. Pat. No. 5,265,221 (Access restriction facility method and apparatus); U.S. Pat. No. 6,161,139 (Win, Administrative Roles that Govern Access to Administrative Functions), each of which is expressly incorporated herein by reference.

John Barkley, Role-Based Access Control for the World Wide Web, at http://hissa.nist.gov/rbac/

Secure Networks

U.S. Pat. No. 5,579,393 (Conner, et al., Nov. 26, 1996), expressly incorporated herein by reference, relates to a system and method for secure medical and dental record interchange, comprising a provider system and a payer system. The provider system includes a digital imager, a processing unit, a data transmission/reception device, and a memory having a provider management unit and a security unit. For each image acquired from the digital imager, the provider management unit generates a unique image ID, and creates an image relation structure having a source indicator, a status indicator, and a copy-from indicator. The provider management unit organizes images into a message for transmission to a payer system. The security unit performs message encryption, image signature generation, and message signature generation. The payer system includes a processing unit, a data transmission/reception device, and a memory having a payer management unit and a security unit. The payer system's security unit validates message signatures and image signatures received. The payer management unit generates a message rejection notification or a message acceptance notification. A method for provider-side secure medical and dental record interchange comprises the steps of: acquiring an image; generating a unique image ID and an image relation structure; maintaining a status indicator, a source indicator, and a copy-from indicator; generating an image signature; creating a message that includes the image; and generating a message signature. A method for payer-side secure medical and dental record interchange comprises the steps of: validating a message signature; validating an image signature; and selectively generating a message acceptance notification or a message rejection notification.

U.S. Pat. No. 5,890,129 (Spurgeon, Mar. 30, 1999), expressly incorporated herein by reference, relates to a system for exchanging health care insurance information. An information-exchange system is provided for controlling the exchange of business and clinical information between an insurer and multiple health care providers. The system includes an information-exchange computer that is connected over a local area network to an insurer computer using a proprietary database and over the Internet to health-care provider computers using open database-compliant databases. The information-exchange computer receives subscriber insurance data from the insurance computer database, translates the insurance data into an exchange database, and pushes the subscriber insurance data out over the Internet to the computer operated by the health-care provider assigned to each subscriber. The information-exchange system stores the data in the provider database. The information-exchange systems also provide for the preparation, submission, processing, and payment of claims over the local area network and with push technology over the Internet. In addition, prior authorization requests may be initiated in the provider computers and exchanged over the information-exchange system for review by the insurer computer. Processed reviews are transmitted back to the provider computer and to a specialist computer, if required, using push technology over the Internet.

U.S. Pat. No. 5,930,759 (Moore, et al., Jul. 27, 1999), expressly incorporated herein by reference, relates to a method and system for processing health care electronic data transactions. A system or network for assembling, filing and processing health care data transactions and insurance claims made by patients pursuant to health care policies issued to the patients by insurance companies or other carriers for service provided to the patients at health care facilities is provided. The network comprises a multitude of participating patients, a multitude of health care facilities, and a plurality of insurance companies or other carriers. Each of the patients has a personal data file including a set of patient related data encoded in a machine readable format, and each of the health care facilities has a telecommunications unit and a file reader to read the data on the personal data files and to transmit the patient related data to the telecommunications unit at the facility. The network further includes a central claims processing unit connected to the telecommunications units of the health care facilities to receive the electronic claim forms from those facilities and to adjudicate those claims.

U.S. Pat. No. 5,933,498 (Schneck, et al., Aug. 3, 1999), expressly incorporated herein by reference, relates to a system for controlling access and distribution of digital property represented as data. Portions of the data are protected and rules concerning access rights to the data are determined. Access to the protected portions of the data is prevented, other than in a non-useable form; and users are provided access to the data only in accordance with the rules

as enforced by a mechanism protected by tamper detection. A method is also provided for distributing data for subsequent controlled use of those data. The method includes protecting portions of the data; preventing access to the protected portions of the data other than in a non-useable form; determining rules concerning access rights to the data; protecting the rules; and providing a package including: the protected portions of the data and the protected rules. A user is provided controlled access to the distributed data only in accordance with the rules as enforced by a mechanism protected by tamper protection. A device is provided for controlling access to data having protected data portions and rules concerning access rights to the data. The device includes means for storing the rules; and means for accessing the protected data portions only in accordance with the rules, whereby user access to the protected data portions is permitted only if the rules indicate that the user is allowed to access the portions of the data.

U.S. Pat. No. 5,978,918 (Scholnick, et al., Nov. 2, 1999), expressly incorporated herein by reference, relates to a practical method and system for supplementing or replacing current security protocols used on public networks involving the distribution of a proprietary system for use on a public network access provider's network. The proprietary system includes processing hardware and proprietary software. The proprietary system transmits private data, outside the Internet, over proprietary lines to a back-end process. When a "sender" sends private data it is sent over the proprietary system to a back-end process. The back-end process returns a time sensitive token that the "sender" sends to the "receiver". The "receiver" takes the time sensitive token and uses it to either retrieve the private data, over a proprietary system, or initiate a transaction with a financial institution. Encryption is used to allow authentication of the participants. This method can be used in conjunction with Secure Socket Layer (SSL) encryption and/or the Secure Electronic Transaction (SET) protocol.

U.S. Pat. No. 6,005,943 (Cohen, et al., Dec. 21, 1999), expressly incorporated herein by reference, relates to electronic identifiers for network terminal devices. The generation of electronic identifiers for network interface units connected to a data network for use in detecting unauthorized decryption of encrypted data transmitted over the data network. A random number is generated for use as a private key decryption code and is stored in memory in each network interface unit. A public key is calculated from the stored private key using a non-invertible mathematical formula. If the calculated public key is unique, then a portion of the public key (e.g. a subset of its bits) is stored in a data provider database as an electronic identifier for use in detecting unauthorized decryption of data by the interface unit.

U.S. Pat. No. 6,009,526 (Choi, Dec. 28, 1999), expressly incorporated herein by reference, relates to an information security system for tracing information outflow from a remotely accessible computer or computer network. The system includes an internal communication system that has at least one internal computer for transmitting security information by tracing data through communication equipment, outputting the data to an external output means, and connecting the internal computer to an external network. A communication monitoring device stores information regarding the data that is to be transmitted by applying a security policy according to a security grade assigned to the destination to which the data is to be transmitted. The communication-monitoring device is configured for extracting the identification of the destination from the transmitted data. It also includes a communication-monitoring server for storing and displaying predetermined information about the data to be transmitted and for determining whether the tracing information is stored according to the security grade for the identified destination. A method of operating the disclosed system is also described.

U.S. Pat. No. 6,021,202 (Anderson, et al., Feb. 1, 2000), expressly incorporated herein by reference, relates to a method and system for processing electronic documents, which includes a markup language according to the SGML standard in which document type definitions are created under which electronic documents are divided into blocks that are associated with logical fields that are specific to the type of block. Each of many different types of electronic documents can have a record mapping to a particular environment, such as a legacy environment of a banking network, a hospital's computer environment for electronic record keeping, a lending institution's computer environment for processing loan applications, or a court or arbitrator's computer system. Semantic document type definitions for various electronic document types (including, for example, electronic checks, mortgage applications, medical records, prescriptions, contracts, and the like) can be formed using mapping techniques between the logical content of the document and the block that is defined to include such content. Also, the various document types are preferably defined to satisfy existing customs, protocols and legal rules.

U.S. Pat. No. 6,021,491 (Renaud, Feb. 1, 2000), expressly incorporated herein by reference, relates to digital signatures for data streams and data archives. Methods, apparatuses and products are provided for verifying the authenticity of data within one or more data files. Each data file is provided with an identifier, such as a one-way hash function or cyclic redundancy checksum. A signature file, that includes the identifiers for one or more data files, is provided with a digital signature created with a signature algorithm. The data file(s) and signature file are then transferred, or otherwise provided to a user. The user verifies the digital signature in the signature file using a signature-verifying algorithm. Once verified as being authentic, the signature file can be used to verify each of the data files. Verification of the data files can be accomplished by comparing the identifier for each data file with the corresponding identifier in the signature file. If the identifiers in the data and signature files match, then the data file can be marked as authentic. If the identifiers do not match then the data file can be rejected or otherwise dealt with accordingly.

U.S. Pat. No. 6,021,497 (Bouthillier, et al., Feb. 1, 2000), expressly incorporated herein by reference, relates to a secured network system which will allow only authorized users of the seed network system to access classified data provided by a secured network server. The secured network system includes a readykey controller, which has connected thereto a plurality of card readers. A user of the secured network system inserts a microchip embedded card into one of the card readers which then provides an authorization signal to the readykey controller indicating that the user is authorized to use one of a plurality of computers within the secured network system to receive and process classified data. The readykey controller sends an enable signal to a data relay switch enabling a data line associated with the card reader and the computer selected by the user allowing classified data to be transmitted from the secured network server through the data relay switch to the selected computer. Each of the three computers also has a power relay switch connected thereto which is activated by the readykey

controller whenever authorization to activate the computer is provided to the readykey controller from another of the plurality of card readers.

U.S. Pat. No. 6,023,762 (Dean, et al., Feb. 8, 2000), expressly incorporated herein by reference, relates to a data access and retrieval system which comprises a plurality of user data sources each storing electronic data signals describing data specific to a user, or enabling services selected by a user; an agent device which is configurable to select individual ones of the user data sources and present selections of user data and service data to a set of callers who may interrogate the agent device remotely over a communications network; a plurality of service terminals capable of communicating with the agent device over a communications network the service terminals operable by callers; and a plurality of key devices, storing caller information and security code information for enabling remote access of selections of user data and/or services to be transmitted over a communications network to a caller located at a service terminal.

U.S. Pat. No. 6,029,245 (Scanlan, Feb. 22, 2000), expressly incorporated herein by reference, relates to a method and system for dynamically assigning security parameters to hypertext markup language (HTML) pages of an information provider on the worldwide web, whereby only one set of HTML pages need be stored and maintained for retrieval by client computers using differing security protocols. A security injection profile is provided for storing security parameters for each respective security protocol. When a browser enabled with a particular security protocol requests one of the HTML pages in the secure set, the page is accessed from web server storage, security parameters of the particular protocol are accessed and injected into the accessed page, and the page is sent to the requesting browser.

U.S. Pat. No. 6,049,875 (Suzuki, et al., Apr. 11, 2000), expressly incorporated herein by reference, relates to a security apparatus and method. A service is supplied to a user while maintaining the security of the service. A person discrimination section discriminates the user to be supplied the service. A user situation decision section decides whether the user is authorized to use the service. An infringement situation decision section detects whether a non-user intrudes into a use area of the service in order to decide whether the security of the service is infringed. A service control section supplies the service to the user in case the person discrimination section discriminates the user, and controls a supply of the service if the use situation decision section decides the user is not under the situation to use the service or the infringement situation decision section decides that the security of the service is infringed.

U.S. Pat. No. 6,055,508 (Naor, et al., Apr. 25, 2000), expressly incorporated herein by reference, relates to a method for secure accounting and auditing on a communications network. A method for secure accounting and auditing of a communications network operates in an environment in which many servers serve an even larger number of clients (e.g. the web), and are required to meter the interaction between servers and clients (e.g. counting the number of clients that were served by a server). The method (metering process) is very efficient and does not require extensive usage of any new communication channels. The metering is secure against fraud attempts by servers that inflate the number of their clients and against clients that attempt to disrupt the metering process. Several secure and efficient constructions of this method are based on efficient cryptographic techniques, are also very accurate, and preserve the privacy of the clients.

U.S. Pat. No. 6,065,119 (Sandford, II, et al., May 16, 2000), expressly incorporated herein by reference, relates to a method of authenticating digital data such as measurements made for medical, environmental purposes, or forensic purpose, and destined for archival storage or transmission through communications channels in which corruption or modification in part is possible. Authenticated digital data contain data-metric quantities that can be constructed from the digital data by authorized persons having a digital key. To verify retrieved or received digital data, the data-metrics constructed from the retrieved or received data are compared with similar data-metrics calculated for the retrieved or received digital data. The comparison determines the location and measures the amount of modification or corruption in the retrieved or received digital data.

U.S. Pat. No. 6,073,240 (Kurtzberg, et al., Jun. 6, 2000), expressly incorporated herein by reference, relates to a method and apparatus for realizing computer security. The method includes the steps of establishing an authorization window for enabling computer system actions consistent with an authorization rule; and, monitoring the actions as an indicia of conformance to the authorization rule. The method preferably provides a pattern of system actions as an indicia of compliance with an authorization rule, and provides notification of predetermined patterns.

U.S. Pat. No. 6,075,860 (Ketcham Jun. 13, 2000), expressly incorporated herein by reference, relates to an apparatus and method for authentication and encryption of a remote terminal over a wireless link. A method and system is provided for authenticating an authorized user of a remote terminal attempting to interconnect with a computer network over a wireless modem is provided. An encrypted wireless communication channel is established between a remote terminal and a network server for facilitating the authentication process. An authorized user presents an authentication card containing credentials including a user identifier and an authentication encryption key to a remote terminal. The remote terminal establishes a wireless communication channel with a network server that provides a firewall between unauthenticated users and a computer network. The network server and the remote terminal then exchange encrypted information thus verifying the authenticity of each party. The remote terminal and the network server each independently generate a data encryption key for use in establishing a secure encrypted wireless communication channel therebetween.

U.S. Pat. No. 6,075,861 (Miller, II, Jun. 13, 2000), expressly incorporated herein by reference, relates to a security access system, having an entry access system that includes a locking mechanism enabling authorized entry at a secured entry point to a closed access area or computing device. Entry is approved in response to an interaction between an intended entrant and the entry access system that involves an interchange of multidigit numbers and use of ID and PINs for generation of a multidigit check number to establish authenticity of a request for entry.

U.S. Pat. No. 6,092,724 (Bouthillier, Secured network system), expressly incorporated herein by reference

Cryptographic Technology

U.S. Pat. No. 5,956,408 (Arnold, Sep. 21, 1999), expressly incorporated herein by reference, relates to an apparatus and method for secure distribution of data. Data, including program and software updates, is encrypted by a public key encryption system using the private key of the

data sender. The sender also digitally signs the data. The receiver decrypts the encrypted data, using the public key of the sender, and verifies the digital signature on the transmitted data. The program interacts with basic information stored within the confines of the receiver. As result of the interaction, the software updates are installed within the confines of the user, and the basic information stored within the confines of the user is changed.

U.S. Pat. No. 5,982,891 (Ginter, et al., Nov. 9, 1999); U.S. Pat. No. 5,949,876 (Ginter, et al., Sep. 7, 1999); and U.S. Pat. No. 5,892,900 (Ginter, et al., Apr. 6, 1999), expressly incorporated herein by reference, relate to systems and methods for secure transaction management and electronic rights protection. Electronic appliances, such as computers, help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-electronic information distribution, for example, utilizing the "electronic highway."

U.S. Pat. No. 6,009,177 (Sudia, Dec. 28, 1999), expressly incorporated herein by reference, relates to a cryptographic system and method with a key escrow feature that uses a method for verifiably splitting users' private encryption keys into components and for sending those components to trusted agents chosen by the particular users, and provides a system that uses modern public key certificate management, enforced by a chip device that also self-certifies. The methods for key escrow and receiving an escrow certificate are also applied herein to a more generalized case of registering a trusted device with a trusted third party and receiving authorization from that party enabling the device to communicate with other trusted devices. Further preferred embodiments provide for rekeying and upgrading of device firmware using a certificate system, and encryption of stream-oriented data.

U.S. Pat. No. 6,052,467 (Brands, Apr. 18, 2000), expressly incorporated herein by reference, relates to a system for ensuring that the blinding of secret-key certificates is restricted, even if the issuing protocol is performed in parallel mode. A cryptographic method is disclosed that enables the issuer in a secret-key certificate issuing protocol to issue triples consisting of a secret key, a corresponding public key, and a secret-key certificate of the issuer on the public key, in such a way that receiving parties can blind the public key and the certificate, but cannot blind a predetermined non-trivial predicate of the secret key even when executions of the issuing protocol are performed in parallel. See, Stefan Brands, Secret Key Certificates, Restrictive Blinding of Secret Key Certificates, Untraceable Off-line Cash in Wallets with Ovservers, and Electronic Cash on the Internet.

U.S. Pat. No. 6,052,780 (Glover, Apr. 18, 2000), expressly incorporated herein by reference, relates to a computer system and process for accessing an encrypted and self-decrypting digital information product while restricting access to decrypted digital information. Some of these problems with digital information protection systems may be overcome by providing a mechanism that allows a content provider to encrypt digital information without requiring either a hardware or platform manufacturer or a content consumer to provide support for the specific form of corresponding decryption. This mechanism can be provided in a manner that allows the digital information to be copied easily for back-up purposes and to be transferred easily for distribution, but which should not permit copying of the digital information in decrypted form. In particular, the encrypted digital information is stored as an executable computer program that includes a decryption program that decrypts the encrypted information to provide the desired digital information, upon successful completion of an authorization procedure by the user. In combination with other mechanisms that track distribution, enforce royalty payments and control access to decryption keys, an improved method is provided for identifying and detecting sources of unauthorized copies. Suitable authorization procedures also enable the digital information to be distributed for a limited number of uses and/or users, thus enabling per-use fees to be charged for the digital information.

See also, U.S. Pat. No. 4,200,770 (Cryptographic apparatus and method); U.S. Pat. No. 4,218,582 (Public key cryptographic apparatus and method); U.S. Pat. No. 4,264,782 (Method and apparatus for transaction and identity verification); U.S. Pat. No. 4,306,111 (Simple and effective public-key cryptosystem); U.S. Pat. No. 4,309,569 (Method of providing digital signatures); U.S. Pat. No. 4,326,098 (High security system for electronic signature verification); U.S. Pat. No. 4,351,982 (RSA Public-key data encryption system having large random prime number generating microprocessor or the like); U.S. Pat. No. 4,365,110 (Multiple-destinational cryptosystem for broadcast networks); U.S. Pat. No. 4,386,233 (Crytographic key notarization methods and apparatus); U.S. Pat. No. 4,393,269 (Method and apparatus incorporating a one-way sequence for transaction and identity verification); U.S. Pat. No. 4,399,323 (Fast real-time public key cryptography); U.S. Pat. No. 4,405,829 (Cryptographic communications system and method); U.S. Pat. No. 4,438,824 (Apparatus and method for cryptographic identity verification); U.S. Pat. No. 4,453,074 (Protection system for intelligent cards); U.S. Pat. No. 4,458,109 (Method and apparatus providing registered mail features in an electronic communication system); U.S. Pat. No. 4,471,164 (Stream cipher operation using public key cryptosystem); U.S. Pat. No. 4,514,592 (Cryptosystem); U.S. Pat. No. 4,528,588 (Method and apparatus for marking the information content of an information carrying signal); U.S. Pat. No. 4,529,870 (Cryptographic identification, financial transaction, and credential device); U.S. Pat. No. 4,558,176 (Computer systems to inhibit unauthorized copying, unauthorized usage, and automated cracking of protected software); U.S. Pat. No. 4,567,600 (Method and apparatus for maintaining the privacy of digital messages conveyed by public transmission); U.S. Pat. No. 4,575,621 (Portable electronic transaction device and system therefor); U.S. Pat. No. 4,578,531 (Encryption system key distribution method and apparatus); U.S. Pat. No. 4,590,470 (User authentication system employing encryption functions); U.S. Pat. No. 4,595,950 (Method and apparatus for marking the information content of an information carrying signal); U.S. Pat. No. 4,625,076 (Signed document transmission system); U.S. Pat. No. 4,633,036 (Method and apparatus for use in public-key data encryption system); U.S. Pat. No. 5,991,406 (System and method for data recovery); U.S. Pat. No. 6,026,379 (System, method and article of manufacture for managing

transactions in a high availability system); U.S. Pat. No. 6,026,490 (Configurable cryptographic processing engine and method); U.S. Pat. No. 6,028,932 (Copy prevention method and apparatus for digital video system); U.S. Pat. No. 6,028,933 (Encrypting method and apparatus enabling multiple access for multiple services and multiple transmission modes over a broadband communication network); U.S. Pat. No. 6,028,936 (Method and apparatus for authenticating recorded media); U.S. Pat. No. 6,028,937 (Communication device which performs two-way encryption authentication in challenge response format); U.S. Pat. No. 6,028,939 (Data security system and method); U.S. Pat. No. 6,029,150 (Payment and transactions in electronic commerce system); U.S. Pat. No. 6,029,195 (System for customized electronic identification of desirable objects); U.S. Pat. No. 6,029,247 (Method and apparatus for transmitting secured data); U.S. Pat. No. 6,031,913 (Apparatus and method for secure communication based on channel characteristics); U.S. Pat. No. 6,031,914 (Method and apparatus for embedding data, including watermarks, in human perceptible images); U.S. Pat. No. 6,034,618 (Device authentication system which allows the authentication function to be changed); U.S. Pat. No. 6,035,041 (Optimal-resilience, proactive, public-key cryptographic system and method); U.S. Pat. No. 6,035,398 (Cryptographic key generation using biometric data); U.S. Pat. No. 6,035,402 (Virtual certificate authority); U.S. Pat. No. 6,038,315 (Method and system for normalizing biometric variations to authenticate users from a public database and that ensures individual biometric data privacy); U.S. Pat. No. 6,038,316 (Method and system for protection of digital information); U.S. Pat. No. 6,038,322 (Group key distribution); U.S. Pat. No. 6,038,581 (Scheme for arithmetic operations in finite field and group operations over elliptic curves realizing improved computational speed); U.S. Pat. No. 6,038,665 (System and method for backing up computer files over a wide area computer network); U.S. Pat. No. 6,038,666 (Remote identity verification technique using a personal identification device); U.S. Pat. No. 6,041,122 (Method and apparatus for hiding cryptographic keys utilizing autocorrelation timing encoding and computation); U.S. Pat. No. 6,041,123 (Centralized secure communications system); U.S. Pat. No. 6,041,357 (Common session token system and protocol); U.S. Pat. No. 6,041,408 (Key distribution method and system in secure broadcast communication); U.S. Pat. No. 6,041,410 (Personal identification fob); U.S. Pat. No. 6,044,131 (Secure digital x-ray image authentication method); U.S. Pat. No. 6,044,155 (Method and system for securely archiving core data secrets); U.S. Pat. No. 6,044,157 (Microprocessor suitable for reproducing AV data while protecting the AV data from illegal copy and image information processing system using the microprocessor); U.S. Pat. No. 6,044,205 (Communications system for transferring information between memories according to processes transferred with the information); U.S. Pat. No. 6,044,349 (Secure and convenient information storage and retrieval method and apparatus); U.S. Pat. No. 6,044,350 (Certificate meter with selectable indemnification provisions); U.S. Pat. No. 6,044,388 (Pseudorandom number generator); U.S. Pat. No. 6,044,462 (Method and apparatus for managing key revocation); U.S. Pat. No. 6,044,463 (Method and system for message delivery utilizing zero knowledge interactive proof protocol); U.S. Pat. No. 6,044,464 (Method of protecting broadcast data by fingerprinting a common decryption function); U.S. Pat. No. 6,044,466 (Flexible and dynamic derivation of permissions); U.S. Pat. No. 6,044,468 (Secure transmission using an ordinarily insecure network communication protocol such as SNMP); U.S. Pat. No. 6,047,051 (Implementation of charging in a telecommunications system); U.S. Pat. No. 6,047,066 (Communication method and device); U.S. Pat. No. 6,047,067 (Electronic-monetary system); U.S. Pat. No. 6,047,072 (Method for secure key distribution over a nonsecure communications network); U.S. Pat. No. 6,047,242 (Computer system for protecting software and a method for protecting software); U.S. Pat. No. 6,047,268 (Method and apparatus for billing for transactions conducted over the internet); U.S. Pat. No. 6,047,269 (Self-contained payment system with circulating digital vouchers); U.S. Pat. No. 6,047,374 (Method and apparatus for embedding authentication information within digital data); U.S. Pat. No. 6,047,887 (System and method for connecting money modules); U.S. Pat. No. 6,049,610 (Method and apparatus for digital signature authentication); U.S. Pat. No. 6,049,612 (File encryption method and system); U.S. Pat. No. 6,049,613 (Method and apparatus for encrypting, decrypting, and providing privacy for data values); U.S. Pat. No. 6,049,671 (Method for identifying and obtaining computer software from a network computer); U.S. Pat. No. 6,049,785 (Open network payment system for providing for authentication of payment orders based on a confirmation electronic mail message); U.S. Pat. No. 6,049,786 (Electronic bill presentment and payment system which deters cheating by employing hashes and digital signatures); U.S. Pat. No. 6,049,787 (Electronic business transaction system with notarization database and means for conducting a notarization procedure); U.S. Pat. No. 6,049,838 (Persistent distributed capabilities); U.S. Pat. No. 6,049,872 (Method for authenticating a channel in large-scale distributed systems); U.S. Pat. No. 6,049,874 (System and method for backing up computer files over a wide area computer network); U.S. Pat. No. 6,052,466 (Encryption of data packets using a sequence of private keys generated from a public key exchange); U.S. Pat. No. 6,052,467 (System for ensuring that the blinding of secret-key certificates is restricted, even if the issuing protocol is performed in parallel mode); U.S. Pat. No. 6,052,469 (Interoperable cryptographic key recovery system with verification by comparison); U.S. Pat. No. 6,055,314 (System and method for secure purchase and delivery of video content programs); U.S. Pat. No. 6,055,321 (System and method for hiding and extracting message data in multimedia data); U.S. Pat. No. 6,055,508 (Method for secure accounting and auditing on a communications network); U.S. Pat. No. 6,055,512 (Networked personal customized information and facility services); U.S. Pat. No. 6,055,636 (Method and apparatus for centralizing processing of key and certificate life cycle management); U.S. Pat. No. 6,055,639 (Synchronous message control system in a Kerberos domain); U.S. Pat. No. 6,056,199 (Method and apparatus for storing and reading data); U.S. Pat. No. 6,057,872 (Digital coupons for pay televisions); U.S. Pat. No. 6,058,187 (Secure telecommunications data transmission); U.S. Pat. No. 6,058,188 (Method and apparatus for interoperable validation of key recovery information in a cryptographic system); U.S. Pat. No. 6,058,189 (Method and system for performing secure electronic monetary transactions); U.S. Pat. No. 6,058,193 (System and method of verifying cryptographic postage evidencing using a fixed key set); U.S. Pat. No. 6,058,381 (Many-to-many payments system for network content materials); U.S. Pat. No. 6,058,383 (Computationally efficient method for trusted and dynamic digital objects dissemination); U.S. Pat. No. 6,061,448 (Method and system for dynamic server document encryption); U.S. Pat. No. 6,061,454 (System, method, and computer program for communicating a key recovery block to enable third party moni-

toring without modification to the intended receiver); U.S. Pat. No. 6,061,692 (System and method for administering a meta database as an integral component of an information server); U.S. Pat. No. 6,061,789 (Secure anonymous information exchange in a network); U.S. Pat. No. 6,061,790 (Network computer system with remote user data encipher methodology); U.S. Pat. No. 6,061,791 (Initial secret key establishment including facilities for verification of identity); U.S. Pat. No. 6,061,792 (System and method for fair exchange of time-independent information goods over a network); U.S. Pat. No. 6,061,794 (System and method for performing secure device communications in a peer-to-peer bus architecture); U.S. Pat. No. 6,061,796 (Multi-access virtual private network); U.S. Pat. No. 6,061,799 (Removable media for password based authentication in a distributed system); U.S. Pat. No. 6,064,723 (Network-based multimedia communications and directory system and method of operation); U.S. Pat. No. 6,064,738 (Method for encrypting and decrypting data using chaotic maps); U.S. Pat. No. 6,064,740 (Method and apparatus for masking modulo exponentiation calculations in an integrated circuit); U.S. Pat. No. 6,064,741 (Method for the computer-aided exchange of cryptographic keys between a user computer unit U and a network computer unit N); U.S. Pat. No. 6,064,764 (Fragile watermarks for detecting tampering in images); U.S. Pat. No. 6,064,878 (Method for separately permissioned communication); U.S. Pat. No. 6,065,008 (System and method for secure font subset distribution); U.S. Pat. No. 6,067,620 (Stand alone security device for computer networks); U.S. Pat. No. 6,069,647 (Conditional access and content security method); U.S. Pat. No. 6,069,952 (Data copyright management system); U.S. Pat. No. 6,069,954 (Cryptographic data integrity with serial bit processing and pseudo-random generators); U.S. Pat. No. 6,069,955 (System for protection of goods against counterfeiting); U.S. Pat. No. 6,069,969 (Apparatus and method for electronically acquiring fingerprint images); U.S. Pat. No. 6,069,970 (Fingerprint sensor and token reader and associated methods); U.S. Pat. No. 6,070,239 (System and method for executing verifiable programs with facility for using non-verifiable programs from trusted sources); U.S. Pat. No. 6,072,870 (System, method and article of manufacture for a gateway payment architecture utilizing a multichannel, extensible, flexible architecture); U.S. Pat. No. 6,072,874 (Signing method and apparatus using the same); U.S. Pat. No. 6,072,876 (Method and system for depositing private key used in RSA cryptosystem); U.S. Pat. No. 6,073,125 (Token key distribution system controlled acceptance mail payment and evidencing system); U.S. Pat. No. 6,073,160 (Document communications controller); U.S. Pat. No. 6,073,172 (Initializing and reconfiguring a secure network interface); U.S. Pat. No. 6,073,234 (Device for authenticating user's access rights to resources and method); U.S. Pat. No. 6,073,236 (Authentication method, communication method, and information processing apparatus); U.S. Pat. No. 6,073,237 (Tamper resistant method and apparatus); U.S. Pat. No. 6,073,238 (Method of securely loading commands in a smart card); U.S. Pat. No. 6,073,242 (Electronic authority server); U.S. Pat. No. 6,075,864 (Method of establishing secure, digitally signed communications using an encryption key based on a blocking set cryptosystem); U.S. Pat. No. 6,075,865 (Cryptographic communication process and apparatus); U.S. Pat. No. 6,076,078 (Anonymous certified delivery); U.S. Pat. No. 6,076,162 (Certification of cryptographic keys for chipcards); U.S. Pat. No. 6,076,163 (Secure user identification based on constrained polynomials); U.S. Pat. No. 6,076,164 (Authentication method and system using IC card); U.S. Pat. No. 6,076,167 (Method and system for improving security in network applications); U.S. Pat. No. 6,078,663 (Communication apparatus and a communication system); U.S. Pat. No. 6,078,665 (Electronic encryption device and method); U.S. Pat. No. 6,078,667 (Generating unique and unpredictable values); U.S. Pat. No. 6,078,909 (Method and apparatus for licensing computer programs using a DSA signature); U.S. Pat. No. 6,079,018 (System and method for generating unique secure values for digitally signing documents); U.S. Pat. No. 6,079,047 (Unwrapping system and method for multiple files of a container); U.S. Pat. No. 6,081,597 (Public key cryptosystem method and apparatus); U.S. Pat. No. 6,081,598 (Cryptographic system and method with fast decryption); U.S. Pat. No. 6,081,610 (System and method for verifying signatures on documents); U.S. Pat. No. 6,081,790 (System and method for secure presentment and payment over open networks); U.S. Pat. No. 6,081,893 (System for supporting secured log-in of multiple users into a plurality of computers using combined presentation of memorized password and transportable passport record), U.S. Pat. No. 6,192,473 (System and method for mutual authentication and secure communications between a postage security device and a meter server), U.S. Pat. No. 6,141,750 (Micali); U.S. Pat. No. 6,137,884 (Micali); U.S. Pat. No. 6,134,326 (Micali); U.S. Pat. No. 6,026,163 (Micali); U.S. Pat. No. 5,812,670 (Micali); U.S. Pat. No. 5,790,665 (Micali); U.S. Pat. No. 5,666,420 (Micali); U.S. Pat. No. 5,666,414 (Micali); U.S. Pat. No. 5,629,982 (Micali); U.S. Pat. No. 5,604,804 (Micali); U.S. Pat. No. 5,553,145 (Micali); U.S. Pat. No. 5,315,658 (Micali); U.S. Pat. No. 5,276,737 (Micali); U.S. Pat. No. 5,519,778 (Leighton et al., (Method for Enabling Users of a Cryptosystem to Generate and use a Private Pair Key for Enciphering Communications Between the Users); U.S. Pat. No. 6,073,242 (Hardy, Electronic Authority Server); U.S. Pat. No. 4,405,829 (Rivest, Cryptographic Communications System and Method); U.S. Pat. No. 4,218,582; U.S. Pat. No. 6,108,644 (Goldschlag, System and Method for Electronic Transactions); U.S. Pat. No. 6,108,787 (Anderson, Method and means for interconnecting different security levels); U.S. Pat. No. 6,151,395 (Harkins, System and method for regenerating secret keys in Diffie-Hellman communication sessions); U.S. Pat. No. 5,949,877 (Traw, Content protection for transmission systems); U.S. Pat. No. 6,072,876 (Obata, Method for Depositing Key in RSA Cryptosystem); U.S. Pat. No. 5,768,388 (Goldwasser, Time Delayed Key Escrow); U.S. Pat. No. 6,158,010 (Moriconi, System and method for maintaining security in a distributed computer network); U.S. Pat. No. 6,148,342 (Ho, Secure Database Management System for Confidential Records Using Separately Encrypted Identifier and Access Request); U.S. Pat. No. 5,920,630 (Wertheimer, Method of public key cryptography that includes key escrow); U.S. Pat. No. 6,119,229 (Martinez, Virtual property system); U.S. Pat. No. 5,745,573 (Lipner, System and Method for Controlling Access to a User Secret); U.S. Pat. No. 5,631,961 (Mills, Device for and Method of Cryptography that Allows Third Party Access); U.S. Pat. No. 6,044,350 (Weiant, Certificate Meter with Selectable Indemnification Provisions); U.S. Pat. No. 5,933,498 (Schneck, System for Controlling Access and Distribution of Digital Property); U.S. Pat. No. 5,737,419 (Ganesan, Computer system for securing communications using split private key asymmetric cryptography); U.S. Pat. No. 6,175,626 (Aucsmith, Digital certificates containing multimedia data extensions); U.S. Pat. No. 6,112,181 (Shear, Systems and methods for matching, selecting, narrowcasting, and/or classifying based on rights management and/or other information); U.S. Pat. No. 6,157,721 (Shear,

Systems and methods using cryptography to protect secure computing environments); U.S. Pat. No. 5,592,549 (Nagel, Method and apparatus for retrieving selected information from a secure information source); U.S. Pat. No. 6,161,181 (Haynes, Secure Electronic Transactions Using a Trusted Intermediary); U.S. Pat. No. 6,145,079 (Mitty, Secure Electronic Transactions Using a Trusted Intermediary to Perform Electronic Services); U.S. Pat. No. 6,118,874 (Okamoto, Encrypted data recovery method using split storage key and system thereof), each of which is expressly incorporated herein by reference.

See, also, U.S. Pat. No. 6,028,937 (Tatebayashi et al.), U.S. Pat. No. 6,026,167 (Aziz), U.S. Pat. No. 6,009,171 (Ciacelli et al.) (Content Scrambling System, or "CSS"), U.S. Pat. No. 5,991,399 (Graunke et al.), U.S. Pat. No. 5,948,136 (Smyers) (IEEE 1394-1995), and U.S. Pat. No. 5,915,018 (Aucsmith), expressly incorporated herein by reference, and Jim Wright and Jeff Robillard (Philsar Semiconductor), "Adding Security to Portable Designs", Portable Design, March 2000, pp. 16–20.

See also, Stefik, U.S. Pat. No. 5,715,403 (System for controlling the distribution and use of digital works having attached usage rights where the usage rights are defined by a usage rights grammar); U.S. Pat. No. 5,638,443 (System for controlling the distribution and use of composite digital works); U.S. Pat. No. 5,634,012 (System for controlling the distribution and use of digital works having a fee reporting mechanism); and U.S. Pat. No. 5,629,980 (System for controlling the distribution and use of digital works), expressly incorporated herein by reference.

See:

Elaine Barker, NIST Cryptographic Toolkit, National Information Security Conference (Oct. 16, 2000); Department of Defense, Trusted Computer System Evaluation Criteria.

Whitfield Diffie and Martin Hellman, Privacy and Authentication: An Introduction to Cryptography at http://www.cs.berkeley.edu/~gribble/osprelims/summaries/priv_auth.html.

Vannevar Bush: As We May Think, Atlantic Monthly, Vol. 176, No. 1, 1945, pp. 101–108, reprinted at http://www.press.umich.edu/jep/works/vbush/vbush-all.html.

Mihir Bellaire and Shafi Goldwasser, Verifiable Partial Key Escrow appearing in Proceedings of the Fourth Annual Conference on Computer and Communications Security, ACM, 1997.

Dorothy Denning, Descriptions of Key Escrow Systems (Version of Feb. 26, 1997) Communications of the ACM (orig. pub. March 1996), reprinted at http://www.cs.georgetown.edu/~denning/crypto/Appendix.html.

Dorothy Denning and Dennis K. Branstad, A Taxonomy for Key Escrow Encryption Systems, Communications of the ACM, vol. 39, No. 3, March 1996 reprinted at http://www.cs.georgetown.edu/~denning/crypto/Taxonomy.html.

A. Michael Froomkin, The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution, 143 University of Pennsylvania Law Review 709–887 (1995).

A. Michael Froomkin, It Came From Planet Clipper: The Battle Over Cryptographic Key "Escrow", 1996 University of Chicago Legal Forum 15–75 (1996).

Lance J. Hoffman, Balanced Key Escrow (Aug. 4, 1995) (GWU-ICTSP-04) printed at ftp://coast.cs.purdue.edu/pub/doc/cryptography/hoffman_balanced_escrow.html.

Wenbo Mao, Verifiable Partial Escrow of Integer Factors (Nov. 16, 2000) citeseer.nj.nec.com/380641.html.

Microsoft Corporation, Encryption and Decryption (Sep. 10, 1996) at http://msdn.microsoft.com/workshop/security/capi/PKCB/crypt4.asp reprinted on 2-10-01.

National Computer Security Center, A Guide to Understanding Discretionary Access Control in Trusted Systems (Sep. 30, 1987) NCSC-TG-003 printed at http://www.certec.or.kr/paper/authent/discretionary_accessi_control.txt.

James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, and Edward Roback, Computer Security Division, NIST, Report on the Development of the Advanced Encryption Standard (Oct. 2, 2000).

Ravi Sandhu, Separation of Duties In Computerized Information Systems (1991), Proceedings of the IFIP WG 11.3 Workshop on Database Security, Halifax, U.K.

Mark Stefik, Trusted Systems, Scientific American, March 1997, pp. 78–81.

Stephen T. Walker, Steven B. Lipner, Carl M. Ellison, Dennis K. Branstad, David M. Balenson. Commercial Key Escrow at http://www.epic.org./crypto/key_escrow/TIS_cke.html

Zero Knowledge Systems, Private Credentials (November 2000).

N. Gilboa, Two Party RSA Key Generation, Proc of Crypto '99, Lecture Notes in Computer Science, Vol. 1666, Springer-Verlag, pp. 116–129, 1999.

D. Boneh, J. Horwitz, \Generating a product of three primes with an unknown factorization ", Proc. of the third Algorithmic Number Theory Symposium (ANTS), 1998, pp. 237–251.

D. Chaum, The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability, Journal of Cryptology, 1/1, 1988, pp. 65–75.

Micali, S.: Fair Public-Key Cryptosystems, Proc. of Crypto '92, LNCS, Springer-Verlag, pp. 113–138 (1993).

M. Bellare and R. Rivest. Translucent cryptography—An alternative to key escrow and its implementation via fractional oblivious transfer. MIT Laboratory for Computer Science Technical Memo. 683, February 1996.

N. Gilboa, Two Party RSA Key Generation, Proc of Crypto '99, Lecture Notes in Computer Science, Vol. 1666, Springer-Verlag, pp. 116–129, 1999.

Rubin, Kerberos Versus the Leighton-Micali Protocol, Dr. Dobb's Journal, November 2000, pages 21–26.

Y. Kun, G. Xin, L. Dayou, Security in Mobile Agent System: Problems and Approaches, Operating Systems Review, 1/2000, 21–28.

C. Ellison, C. Hall, R. Milbert, and B. Schneier. Protecting secret keys with personal entropy. Future Generation Computer Systems, 16(4):311–318, 2000. Available at http://www.counterpane.com/.

E. Dawson, A. Clark, M. Looi, Key management in a non-trusted distributed environment, Future Generation Computer Systems 16 (2000) 319–329.

D. Gollmann, New paradigms-old paradigms?, Future Generation Computer Systems 16 (2000) 343–349.

P. Sklavos, A. Varvitsiotis, D. Polemi, Securing Large E-Commerce Networks, Information Security and Privacy, 5th Australasian Conference, ACISP 2000, Brisbane, Australia, Jul. 10–12, 2000, Proceedings.

Josang, I. Pedersen, D. Povey, PKI Seeks a Trusting Relationship, Information Security and Privacy, 5th Australasian Conference, ACISP 2000, Brisbane, Australia, Jul. 10–12, 2000, Proceedings.

E. F. Brickell. A fast modular multiplication algorithm with application to two key cryptography. In D. Chaum, R. L.

Rivest, and A. T. Sherman, editors, Advances in Cryptology, Proceedings of Crypto 82, pages 51–60. New York, N.Y.: Plenum Press, 1982.

B. Crispo, P. Landrock, V. Matyas, WWW security and trusted third party services, Future Generation Computer Systems 16 (2000) 331–341.

S. Ng, Comments on "On the Security of Three-Party Cryptographic Protocols" by Xu, Zhang and Zhu, Operating Systems Review, Volume 33, Number 3, July 1999, pages 5–13.

Xu, S., Zhang, G. and Zhu, H. On the Security of Three-Party Cryptographic Protocols. Operating Systems Review, 32, 3 (July 1998) 7–20. 2

M. Bellare, "Practice-oriented provable-security," Proceedings of the ISW 97 conference, to appear in Springer Verlag LLNCS, 1998.

Y. Lindell, Privacy Preserving Data Mining, Advances in Cryptology-CRYPTO 2000, 20th Annual International Cryptology Conference Santa Barbara, Calif., USA, Aug. 20–24, 2000 Proceedings.

P. Beauchemin, A Generalization of Hellman's Extension of Shannon's Approach to Cryptography, Advances in Cryptology-CRYPTO '87, Lecture Notes in Computer Science.

P. Wing, Using Public-Key infrastructures for Security and Risk Management, IEEE Communications Magazine, September 1999, pages 71–73.

Bennett, Charles H., Francois Bessette, Gilles Brassard, Louis Salvail, and John Smolin, Experimental quantum cryptography, J. Cryptology (1992) 5: 3–28.

M. Fischer, S. Micali, and C. Rackoff, A Secure Protocol for the Oblivious Transfer, Eurocrypt 1984.

J. Brandt, I. Damgard, P. Landrock, and T. Pedersen, Zero-knowledge authentication scheme with secrete key exchange, Advances in Cryptology: Proceedings of Crypto '88, S. Goldwasser, ed., Lecture Notes in Computer Science 403, Springer-Verlag (1989), 583–588.

Thomas C. Rindfleisch: Privacy, Information Technology, and Health Care; Comm. ACM; Vol. 40 No. 8, Aug. 1997, pp. 92–100.

Charles Pfleeger and Deborah Cooper. Security and Privacy: Promising Advances. IEEE Software, pages 27–32, September/October 1997.

R. Frank, Security Issues in the Virtual Corporation, Computer Fraud & Security, 15 (1996) 471–476.

L. F. Cranor. Internet privacy, Communications of the ACM 42(2), pp. 28–38, February 1999.

Michael Reiter and Aviel Rubin. Anonymous web transactions with crowds. Communications of the ACM, 42(2): 32–38, 1999.

E. Gabber, P. Gibbons, D. Kristol, Y. Matias, and A. Mayer. Consistent, yet anonymous web access with LPWA. Communications of the ACM, 42(2):42–47, February 1999.

J. Reagle and L. Cranor. The platform for privacy preferences. Communications of the ACM, February 1999, vol. 42, n. 2, http://www.w3.org/TR/NOTE-P3P-CACM/.

Paola Benassi. Truste: an online privacy seal program. Comm. ACM, 42(2):56–59, February 1999.

Roger Clarke, "Internet Privacy Concerns Confirm the Case for Intervention", Communications of the ACM, Vol. 42, No. 2, February 1999, pp. 60–67

The AES Candidates, Dr. Dobb's Journal, December 1998, page 36.

Michael Willett, Features, Attributes, Characteristics, and Traits (FACTs) of Key Recovery Schemes/Products, Computers & Security, Vol. 19, No. 1, pages 28–39.

S. Gupta, A Common Key Recovery Block Format: Promoting Interoperability Between Dissimilar Key Recovery Mechanisms, Computers & Security, 19 (2000) 41–47.

M. Smith, P. VanOorschot, M. Willett, Cryptographic Information Recovery Using Key Recovery, Computers & Security, 19 (2000) 21–27.

S. Gupta, S. Matyas, Public Key Infrastructure: Analysis of Existing and Needed Protocols and Object Formats for Key Recovery, Computers & Security, Vol. 19, No. 1, 56–69.

Kh, A. Jabri, The unicity distance: An upper bound on the probability of an eavesdropper successfully estimating the secret key, Information Processing Letters 60 (1996) 4347.

Jose Pastor. CRYPTOPOST: A cryptographic application to mail processing. Journal of Cryptology, 3(2), 1991.

S. Hinde, 2001: A Privacy Odyssey, Computers & Security, 20 (2001) 21–27

M. Joye, S. Yen, ID-based Secret-Key Cryptography, pages 33–39.

Cramer R., Damgard I. and Maurer U., "General Secure Multi-Party Computation from any Linear Secret-Sharing Scheme", manuscript, 1999.

R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Robust and efficient sharing of RSA functions. In Advances in Cryptology—Crypto '96, pages 157–172, 1996.

D. Boneh, M. Franklin. "Efficient generation of shared RSA keys", in Proceedings Crypto '97, pp. 425–439.

Y. Frankel, P. MacKenzie, M. Yung, "Robust efficient distributed RSA key generation", Symposium on Principles of Distributed Computing, page 320, 1998.

Guillaume Poupard and Jacques Stern. Generation of shared rsa keys by two parties. In ASIACRYPT '98, pages 11–24. Springer-Verlag LNCS 1514, 1998.

Simon Blackburn, Simon Blake-Wilson, Mike Burmester, and Steven Galbraith, Shared generation of shared RSA keys, Technical Report CORR98-19, Department of Combinatorics & Optimization, University of Waterloo, 1998.

Cr'epeau Claude, and Joe Kilian, "Achieving Oblivious Transfer Using Weakened Security Assumptions," to appear in Proceedings of the 29 th FOCS, IEEE, 1988.

D. Boneh and M. Franklin Efficient Generation of Shared RSA Keys, Crypto 97 (these proceedings).

R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Robust and efficient sharing of RSA functions. In Advances in Cryptology—Crypto '96, pages 157–172, 1996.

J. Grantham, "A probable prime test with high confidence", http://www.clark.net/pub/grantham/pseudo/

S. Spalding and R. Wright. Experimental Performance of Shared RSA Modulus Generation. In proc. of Algorithms and Experiments 98, pages 34–43, 1998.

S. Spalding and R. Wright. Experimental Performance of Shared RSA Modulus Generation. In proc. of Algorithms and Experiments 98, pages 34–43, 1998.

M. Malkin, T. Wu, and D. Boneh. Experimenting with shared generation of RSA keys. In Proceedings of the Internet Society's 1999 Symposium on Network and Distributed System Security (SNDSS), 1999, pp. 43–56.

R. Cramer, Introduction to Secure Computation, Lectures on Data Security, Modern Cryptology in Theory and Practice, 16–62.

I. Damgard, Commitment Schemes and Zero-Knowledge Protocols, LNCS-1561, 1999, pp. 63–86.

C. Lin, H. Sun, T. Hwang, Three-party Encrypted Key Exchange: Attacks and A Solution

B. Kaliski. Emerging Standards for Public-Key Cryptography, Lectures on Data Security, Modern Cryptology in Theory and Practice, 87–104

A. Beimel, M. Burmester, Y. Desmedt, E. Kushilevitz, Computing Functions of a Shared Secret, SIAM J. on Discrete Mathematics, 13(3):324–345, 2000.

G. Durfee and P. Nguyen, Cryptanalysis of the RSA Schemes with Short Secret Exponent from Asiacrypt '99, Proceedings of Asiacrypt '2000, Dec. 3–7, 2000, Kyoto Japan

V. Phan, Attacks on the RSA Cryptosystem and Some of Its Instances

Tri Van Le and Khanh Quoc Nguyen and Vijay Varadharajan, "How to Prove That a Committed Number is Prime", ASIACRYPT(1999), pp. 208–218.

Watermarking

U.S. Pat. No. 5,699,427 (Chow, et al., Dec. 16, 1997), expressly incorporated herein by reference, relates to a method to deter document and intellectual property piracy through individualization, and a system for identifying the authorized receiver of any particular copy of a document. More specifically, each particular copy of a document is fingerprinted by applying a set of variations to a document, where each variation is a change in data contents, but does not change the meaning or perusal experience of the document. A database associating a set of variants to a receiver is maintained. Thus any variant or copy of that variant can be traced to an authorized receiver.

See also, U.S. Pat. No. 4,734,564 (Transaction system with off-line risk assessment); U.S. Pat. No. 4,812,628 (Transaction system with off-line risk assessment); U.S. Pat. No. 4,926,325 (Apparatus for carrying out financial transactions via a facsimile machine); U.S. Pat. No. 5,235,166 (Data verification method and magnetic media therefor); U.S. Pat. No. 5,254,843 (Securing magnetically encoded data using timing variations in encoded data); U.S. Pat. No. 5,341,429 (Transformation of ephemeral material); U.S. Pat. No. 5,428,683 (Method and apparatus for fingerprinting and authenticating magnetic media); U.S. Pat. No. 5,430,279 (Data verification method and magnetic media therefor); U.S. Pat. No. 5,521,722 (Image handling facilitating computer aided design and manufacture of documents); U.S. Pat. No. 5,546,462 (Method and apparatus for fingerprinting and authenticating various magnetic media); U.S. Pat. No. 5,606,609 (Electronic document verification system and method); U.S. Pat. No. 5,613,004 (Steganographic method and device); U.S. Pat. No. 5,616,904 (Data verification method and magnetic media therefor); U.S. Pat. No. 5,636,292 (Steganography methods employing embedded calibration data); U.S. Pat. No. 5,646,997 (Method and apparatus for embedding authentication information within digital data); U.S. Pat. No. 5,659,726 (Data embedding); U.S. Pat. No. 5,664,018 (Watermarking process resilient to collusion attacks); U.S. Pat. No. 5,687,236 (Steganographic method and device); U.S. Pat. No. 5,710,834 (Method and apparatus responsive to a code signal conveyed through a graphic image); U.S. Pat. No. 5,727,092 (Compression embedding); U.S. Pat. No. 5,734,752 (Digital watermarking using stochastic screen patterns); U.S. Pat. No. 5,740,244 (Method and apparatus for improved fingerprinting and authenticating various magnetic media); U.S. Pat. No. 5,745,569 (Method for stega-cipher protection of computer code); U.S. Pat. No. 5,745,604 (Identification/authentication system using robust, distributed coding); U.S. Pat. No. 5,748,763 (Image steganography system featuring perceptually adaptive and globally scalable signal embedding); U.S. Pat. No. 5,748,783 (Method and apparatus for robust information coding); U.S. Pat. No. 5,761,686 (Embedding encoded information in an iconic version of a text image); U.S. Pat. No. 5,765,152 (System and method for managing copyrighted electronic media); U.S. Pat. No. 5,768,426 (Graphics processing system employing embedded code signals); U.S. Pat. No. 5,778,102 (Compression embedding); U.S. Pat. No. 5,790,703 (Digital watermarking using conjugate halftone screens); U.S. Pat. No. 5,819,289 (Data embedding employing degenerate clusters of data having differences less than noise value); U.S. Pat. No. 5,822,432 (Method for human-assisted random key generation and application for digital watermark system); U.S. Pat. No. 5,822,436 (Photographic products and methods employing embedded information); U.S. Pat. No. 5,832,119 (Methods for controlling systems using control signals embedded in empirical data); U.S. Pat. No. 5,841,886 (Security system for photographic identification); U.S. Pat. No. 5,841,978 (Network linking method using steganographically embedded data objects); U.S. Pat. No. 5,848,155 (Spread spectrum watermark for embedded signalling); U.S. Pat. No. 5,850,481 (Steganographic system); U.S. Pat. No. 5,862,260 (Methods for surveying dissemination of proprietary empirical data); U.S. Pat. No. 5,878,137 (Method for obtaining authenticity identification devices for using services in general, and device obtained thereby); U.S. Pat. No. 5,889,868 (Optimization methods for the insertion, protection, and detection of digital watermarks in digitized data); U.S. Pat. No. 5,892,900 (Systems and methods for secure transaction management and electronic rights protection); U.S. Pat. No. 5,905,505 (Method and system for copy protection of on-screen display of text); U.S. Pat. No. 5,905,800 (Method and system for digital watermarking); U.S. Pat. No. 5,915,027 (Digital watermarking); U.S. Pat. No. 5,920,628 (Method and apparatus for fingerprinting and authenticating various magnetic media); U.S. Pat. No. 5,930,369 (Secure spread spectrum watermarking for multimedia data); U.S. Pat. No. 5,933,498 (System for controlling access and distribution of digital property); U.S. Pat. No. 5,943,422 (Steganographic techniques for securely delivering electronic digital rights management control information over insecure communication channels); U.S. Pat. No. 5,946,414 (Encoding data in color images using patterned color modulated image regions); U.S. Pat. No. 5,949,885 (Method for protecting content using watermarking); U.S. Pat. No. 5,974,548 (Media-independent document security method and apparatus); U.S. Pat. No. 5,995,625 (Electronic cryptographic packing); U.S. Pat. No. 6,002,772 (Data management system); U.S. Pat. No. 6,004,276 (Open architecture cardiology information system); U.S. Pat. No. 6,006,328 (Computer software authentication, protection, and security system); U.S. Pat. No. 6,006,332 (Rights management system for digital media); U.S. Pat. No. 6,018,801 (Method for authenticating electronic documents on a computer network); U.S. Pat. No. 6,026,193 (Video steganography); U.S. Pat. No. 6,044,464 (Method of protecting broadcast data by fingerprinting a common decryption function); U.S. Pat. No. 6,047,374 (Method and apparatus for embedding authentication information within digital data); U.S. Pat. No. 6,049,627 (Covert digital identifying indicia for digital image); U.S. Pat. No. 6,061,451 (Apparatus and method for receiving and decrypting encrypted data and protecting decrypted data from illegal use); U.S. Pat. No. 6,064,737 (Anti-piracy system for wireless telephony); U.S. Pat. No. 6,064,764 (Fragile watermarks for detecting tampering in images); U.S. Pat. No. 6,069,914 (Watermarking of image data using MPEG/JPEG coefficients); U.S. Pat. No. 6,076,077 (Data management system); U.S. Pat. No. 6,081,793 (Method and system for

secure computer moderated voting), each of which is expressly incorporated herein by reference.

Computer System Security

U.S. Pat. No. 5,881,225 (Worth, Mar. 9, 1999), expressly incorporated herein by reference, relates to a security monitor for controlling functional access to a computer system. A security monitor controls security functions for a computer system. A user desiring access to the system inputs a user identification and password combination, and a role the user to assume is selected from among one or more roles defined in the system. Upon being validated as an authorized user performing a particular role, the user is then authorized to perform certain functions and tasks specifically and to see information associated with that role (and optimally the work group the user is assigned). For some users, no role or a "null" roll is chosen, and authorization for certain functions and tasks is accomplished due to that particular user having been predefined by an administrator as being allowed to perform those functions and tasks, usually due to the predefined privileges associated with the work group(s) to which the user belongs.

U.S. Pat. No. 5,937,068 (Audebert, Aug. 10, 1999), expressly incorporated herein by reference, relates to a system and method for user authentication employing dynamic encryption variables. The system includes a first card-like unit adapted to communicate with a second unit giving only conditionally access to a function. Both units are capable of running software for generating a password by means of encryption of a plurality of dynamic variables produced separately but in concert (so as to have a predetermined relationship, such as identity, with one another) in the units. The encryption is carried out in each unit by a public algorithm using a dynamically varying encryption key. Each time an access request is issued by a card user, the key is modified as a function of the number of access requests previously formulated by the card user. Access to the function is granted when the passwords generated in the units have a predetermined relationship (such as identity) with each other. In a "virtual token" implementation, the first unit can be a smart card, which stores the dynamic key and the variable representing the number of formulated authentication requests and executes an encryption algorithm, a smart card reader and a computer such as a personal computer. Either the smart card reader or the personal computer can generate the time dependent variable. In a "software token" implementation, the functions of the first unit are performed by a personal computer, thus eliminating the need for a smart card or a smart card reader.

U.S. Pat. No. 5,949,882 (Angelo, Sep. 7, 1999), expressly incorporated herein by reference, relates to a method and apparatus for allowing access to secured computer resources bar utilizing a password and an external encryption algorithm. A method for permitting access to secured computer resources based upon a two-piece user verification process is provided. In one embodiment, the user verification process is carried out during a secure power-up procedure. At some point during the secure power-up procedure, the computer user is required to provide an external token or smart card that is coupled to the computer through specialized hardware. The token or smart card is used to store an encryption algorithm furnished with an encryption key that is unique or of limited production. The computer user is then required to enter a plain text user password. Once entered, the user password is encrypted using the encryption algorithm contained in the external token to create a peripheral password. The peripheral password is compared to a value stored in either secure system memory or in memory contained within a secured resource itself. If the two values match, access to the secured resource is permitted. In an alternate embodiment, the two-piece authentication process is conducted during normal computer operation outside of the secure power-on sequence. In this embodiment, the user password is entered by means of a secure keyboard communications channel. In either embodiment, the two-piece nature of the authorization process requires the presence of both the user password and the external token in order to generate the peripheral password.

U.S. Pat. No. 5,953,419 (Lohstroh, et al., Sep. 14, 1999), expressly incorporated herein by reference, relates to a cryptographic file labeling system for supporting secured access by multiple users. A system is disclosed for automatically distributing secured versions of a file decryption key to a plurality of file users by way of the file's security label. The label is defined to contain a plurality of Access-Control-Entries Records (ACER's) where each ACER includes a respective secured version of the file decryption key. Each such secured version is decipherable by a respective ACER private key. Each ACER may include respective other data such as: (a) ACER-unique identifying data for uniquely identifying the ACER or an associated user; (b) decryption algorithm identifying data for identifying the decryption process to be used to decrypt the encrypted data portion of the file; and (c) special handling code for specifying special handling for the code-containing ACER. The label is preferably covered by a digital signature but includes an extension buffer that is not covered by the digital signature. Users who wish to have an ACER of their own added to the label may submit add-on requests by writing to the extension buffer.

U.S. Pat. No. 5,956,400 (Chaum, et al., Sep. 21, 1999), expressly incorporated herein by reference, relates to partitioned information storage systems with controlled retrieval. An information storage system includes one or more information update terminals, a mapper, one or more partial-databases, and one or more query terminals, exchanging messages over a set of communication channels. An identifier-mapping mechanism provides (to an update terminal) a method for delegating control over retrieval of the data stored at the partial-databases to one or more mappers, typically operated by one or more trusted third parties. Update terminals supply information, which is stored in fragmented form by the partial-databases. Data-fragment identifiers and pseudonyms are introduced, preventing unauthorized de-fragmentation of information—thus providing compliance to privacy legislation—while at the same time allowing query terminals to retrieve (part of) the stored data or learn properties of the stored data. The mapper is necessarily involved in both operations, allowing data access policies to be enforced and potential abuse of stored information to be reduced. Introduction of multiple mappers acts to distribute information retrieval control among multiple trusted third parties. Introducing so-called "groupers" increases the efficiency of data retrieval for a common set of queries and further reduces potential abuse of information. See, See, David Chaum, Achieving Electronic Privacy, Scientific American, August 1992, p. 96–101.

U.S. Pat. No. 5,958,050 (Griffin, et al., Sep. 28, 1999), expressly incorporated herein by reference, relates to a trusted delegation system. A trust manager examines each new class before it is allowed to execute by examining a policy file which includes data structures defining security policies of the user system, a certificate repository for storing a plurality of certificates, a certificate being a data record which is digitally signed and which certifies claims

relevant to a security evaluation, a code examiner adapted to analyze the portion of code to determine potential resource use of the portion of code and a trust evaluator adapted to evaluate certificate requirements of the portion of code based on policy rules extracted from the policy file and the potential resource use specified by the code examiner. The trust evaluator also determines, from certificates from the certificate repository and a code identifier identifying the portion of code, whether execution of the portion of code is allowed by the policy rules given the potential resource use, the code supplier and applicable certificates. Certificates and policies can be specified in hierarchical form, so that some levels of security can be delegated to trusted entities.

U.S. Pat. No. 5,978,475 (Schneier, et al., Nov. 2, 1999), expressly incorporated herein by reference, relates to an event auditing system. In many computer applications, sensitive information must be kept on an untrusted machine. Such information must be protected against attackers, as well as against partially trusted entities to be given partial, but not total, access to the stored information. A method, apparatus and computer-readable data structure are provided for inhibiting an attacker from accessing or corrupting information stored by an untrusted machine. More specifically, in a log file generated during a process in which the untrusted machine is in limited communication with a trusted machine, entries generated prior to the attack remain secure (they cannot be modified without detection), even though subsequent entries can not be trusted. One embodiment also allows a partially trusted verifier to read and verify entries in the log file, but not to change them without detection. In another embodiment, operating with or without the trusted machine, the untrusted machine's log file can also incorporate log files of other processes.

U.S. Pat. No. 5,991,878 (McDonough, et al., Nov. 23, 1999), expressly incorporated herein by reference, relates to a system and method for controlling access to information in a distributed computing system. A request for the information is received and is accompanied by encrypted session state data. Based on the encrypted session state data, it is determined whether to pass the request on to a source of the information. In a memory buffer, old data is replaced by overwriting with a unique identifier. After the memory buffer has received new data and a procedure has been executed for copying the contents of the memory buffer to a destination, it is determined whether the unique identifier may be found at the destination.

U.S. Pat. No. 6,070,239 (McManis, May 30, 2000), expressly incorporated herein by reference, relates to a system and method for executing verifiable programs with facility for using non-verifiable programs from trusted sources. A computer system includes a program executer that executes verifiable architecture neutral programs and a class loader that prohibits the loading and execution of non-verifiable programs unless (A) the non-verifiable program resides in a trusted repository of such programs, or (B) the non-verifiable program is indirectly verifiable by way of a digital signature on the non-verifiable program that proves the program was produced by a trusted source. In the preferred embodiment, verifiable architecture neutral programs are Java bytecode programs whose integrity is verified using a Java bytecode program verifier. The non-verifiable programs are generally architecture specific compiled programs generated with the assistance of a compiler. Each architecture specific program typically includes two signatures, including one by the compiling party and one by the compiler. Each digital signature includes a signing party identifier and an encrypted message. The encrypted message includes a message generated by a predefined procedure, and is encrypted using a private encryption key associated with the signing party. A digital signature verifier used by the class loader includes logic for processing each digital signature by obtaining a public key associated with the signing party, decrypting the encrypted message of the digital signature with that public key so as generate a decrypted message, generating a test message by executing the predefined procedure on the architecture specific program associated with the digital signature, comparing the test message with the decrypted message, and issuing a failure signal if the decrypted message digest and test message digest do not match.

U.S. Pat. No. 6,079,021 (Abadi, et al., Jun. 20, 2000), expressly incorporated herein by reference, relates to a method and apparatus for strengthening passwords for protection of computer systems. A computer-implemented method provides access to processes and data using strengthened password. During an initialization phase, an access code is stored in a memory of a computer system. The access code is an application of a one-way hash function to a concatenation of a password and a password supplement. The size of the password supplement is a fixed number of bits. During operation of the system, a user enters a password, and the one-way hash function is applied to concatenations of the password and possible values having the size of the password supplement to yield trial access codes. Access is granted when one of the trial access codes is identical to the stored access code.

See:

U.S. Pat. No. 6,141,758 (Banantar, Method and system for maintaining client server associations in a distributed computing system), expressly incorporated herein by reference.

M. Abadi, M. Burrows, B. Lampson, G. Plotkin A Calculus for Access Control in Distributed Systems

Computer Security Devices

U.S. Pat. No. 5,982,520 (Weiser, et al., Nov. 9, 1999), expressly incorporated herein by reference, relates to a personal storage device for receipt, storage, and transfer of digital information to other electronic devices has a pocket sized crush resistant casing with a volume of less than about ten cubic centimeters. A processor is positioned within the casing cavity and attached to the crush resistant casing, while a memory module also positioned within the casing cavity is configured to store received executable applications and data. An infrared transceiver is mounted on the crush resistant casing and in electronic communication with the processor and memory module to provide for receipt and storage of executable applications, and receipt, storage, and transfer of digital information to other electronic devices. The digital information stored by the personal storage device can be intermittently synchronized with other electronic devices.

U.S. Pat. No. 5,991,519 (Benhammou, et al., Nov. 23, 1999), expressly incorporated herein by reference, relates to a secure memory having multiple security levels. A secured memory comprises a first level security zone having an access code controlling access to the secured memory prior to an issuer fuse being blown, a security code attempts counter preventing access to the secured memory when a predetermined number of attempts at matching the access code have been made prior to resetting the security code attempts counter, a plurality of application zones, each of the plurality of application zones comprising: a storage memory zone, an application security zone having an application zone access code controlling access to the storage memory

zone after an issuer fuse has been blown, an application zone security code attempts counter preventing access to the application zone when a predetermined number of attempts at matching the application zone access code have been made prior to resetting the application zone security code attempts counter, an erase key partition having an erase key code controlling erase access to the storage memory zone after an issuer fuse has been blown, and an erase key attempts counter preventing erase access to the application zone when a predetermined number of attempts at matching the erase key code have been made prior to resetting the erase key attempts counter.

U.S. Pat. No. 5,999,629 (Heer, et al., Dec. 7, 1999), expressly incorporated herein by reference, relates to a data encryption security module. Encryption keys used to encrypt such messages need to be managed in a highly secure manner. A unique device encryption key is generated, a cryptographic key formed from a unique identification key and an associated public key, and at least one program encryption key, in which the public key is generated as a function of the unique identification key. The module then encrypts the unique identification key and program encryption key using said device encryption key and stores the encrypted result in memory internal to security module, thereby securing the keys against misappropriation. In addition, the module provides a mechanism for using the program encryption key to encrypt information that it receives from an external source and store the encrypted information in memory external to the security module, and responsive to receiving from a requester a request for the program encryption key, encrypting the program encryption key, using a symmetrical encryption key generated as a function of a public key generated by a security module associated with the requester. The former security module then supplies the encrypted program encryption key to the requester.

U.S. Pat. No. 6,034,618 (Tatebayashi, et al., Mar. 7, 2000), expressly incorporated herein by reference, relates to a device authentication system that allows the authentication function to be changed. A decoder apparatus generates a random number for authenticating the optical disc drive apparatus and sends it to the optical disc drive apparatus as the challenge data. The optical disc drive apparatus selects one out of sixteen claimant functions stored in the claimant function unit and calculates the function value, which it sends to the decoder apparatus as the response data. The decoder apparatus compares the response data with sixteen function values to that are obtained using the sixteen verification functions stored in the verification function unit, and authenticates the optical disc drive apparatus when at least one of the function values matches the response data.

U.S. Pat. No. 6,041,412 (Timson, et al., Mar. 21, 2000), expressly incorporated herein by reference, relates to an apparatus and a method for providing access to a secured data or area, includes at least two secure data modules which contain security data and other information and which belong to a particular security scheme and a dual module reader for reading data and permissions instructions contained on the secure data modules. The two secure data modules include an enabling module and an interrogatable module. The interrogatable module and the enabling module communicate with each other via a dual module reader. Communication between the two modules is allowed as long as the two modules are members of the same security scheme. A scheme is defined by suitable proprietary encryption keys for enabling communication and data transfer between the two modules belonging to a common scheme and for preventing communication and data transfer between two modules belonging to different schemes. The communication between the two modules provides an improved data security and access control system that eliminates the need for multiple passwords for various operations and also prevents problems associated with conventional access cards that are used in conjunction with passwords.

U.S. Pat. No. 6,061,451 (Muratani, et al., May 9, 2000), expressly incorporated herein by reference, relates to an apparatus and method for receiving and decrypting encrypted data and protecting decrypted data from illegal use. A data receiving apparatus is formed of a set top unit connected to a network and a security module. Digital video data, supplied from the network and scrambled according to a first system, is scrambled according to a second system in a scramble circuit in the set top unit, and is supplied to the security module. The data is descrambled according to the first system in a descramble circuit in the security module, and is transferred back to the set top unit. The data is descrambled according to the second system in a descramble circuit in the set top unit, and is outputted to an image display terminal via an MPEG decoder.

U.S. Pat. No. 6,069,647 (Sullivan, et al., May 30, 2000), expressly incorporated herein by reference, relates to a conditional access and content security method. An interface unit, connected to a programmable unit, is capable of containing a time-sensitive key. The programmable unit is allowed to receive digital content from the interface unit upon establishing that the time-sensitive key is also contained therein.

See, U.S. Pat. No. 6,131,090 (Basso, Method and system for providing controlled access to information stored on a portable recording medium); and U.S. Pat. No. 6,125,186 (Saito, Encryption Communication System Using an Agent and a Storage Medium for that Agent), expressly incorporated herein by reference.

Computer Network Firewall

U.S. Pat. No. 5,944,823 (Jade, et al., Aug. 31, 1999), expressly incorporated herein by reference, relates to a system and method for providing outside access to computer resources through a firewall. A firewall isolates computer and network resources inside the firewall from networks, computers and computer applications outside the firewall. Typically, the inside resources could be privately owned databases and local area networks (LAN's), and outside objects could include individuals and computer applications operating through public communication networks such as the Internet. Usually, a firewall allows for an inside user or object to originate connection to an outside object or network, but does not allow for connections to be generated in the reverse direction; i.e. from outside in. The system provides a special "tunneling" mechanism, operating on both sides of a firewall, for establishing such "outside in" connections when they are requested by certain "trusted" individuals or objects or applications outside the firewall. The intent here is to minimize the resources required for establishing "tunneled" connections (connections through the firewall that are effectively requested from outside), while also minimizing the security risk involved in permitting such connections to be made at all. The mechanism includes special tunneling applications, running on interface servers inside and outside the firewall, and a special table of "trusted sockets" created and maintained by the inside tunneling application. Entries in the trusted sockets table define objects inside the firewall consisting of special inside ports, a telecommunication protocol to be used at each port, and a host object associated with each port. Each entry is "trusted" in the sense that it is supposedly known only by

individuals authorized to have "tunneling" access through the firewall from outside. These applications use the table to effect connections through the firewall in response to outside requests identifying valid table entries.

U.S. Pat. No. 5,968,176 (Nessett, et al., Oct. 19, 1999), expressly incorporated herein by reference, relates to a multilayer firewall system. A system provides for establishing security in a network that includes nodes having security functions operating in multiple protocol layers. Multiple network devices, such as remote access equipment, routers, switches, repeaters and network cards having security functions are configured to contribute to implementation of distributed firewall functions in the network. By distributing firewall functionality throughout many layers of the network in a variety of network devices, a pervasive firewall is implemented. The pervasive, multilayer firewall includes a policy definition component that accepts policy data that defines how the firewall should behave. The policy definition component can be a centralized component, or a component that is distributed over the network. The multilayer firewall also includes a collection of network devices that are used to enforce the defined policy. The security functions operating in this collection of network devices across multiple protocol layers are coordinated by the policy definition component so that particular devices enforce that part of the policy pertinent to their part of the network.

U.S. Pat. No. 5,983,350 (Minear, et al., Nov. 9, 1999), expressly incorporated herein by reference, relates to a secure firewall supporting different levels of authentication based on address or encryption status. A system and method is provided for regulating the flow of messages through a firewall having a network protocol stack, wherein the network protocol stack includes an Internet Protocol (IP) layer, the method comprising establishing a security policy, determining, at the IP layer, if a message is encrypted, if the message is not encrypted, passing the unencrypted message up the network protocol stack to an application level proxy, and if the message is encrypted, decrypting the message and passing the decrypted message up the network protocol stack to the application level proxy, wherein decrypting the message includes executing a process at the IP layer to decrypt the message.

U.S. Pat. No. 6,009,475 (Shrader, Dec. 28, 1999), expressly incorporated herein by reference, relates to a system and method for filter rule validation and administration for firewalls. Filter rules on a firewall between a secure computer network and a nonsecure computer network are validated from a user interface. A user interface is presented in which a test packet can be defined. The user interface includes controls for defining values for attributes of the test packet, wherein the attributes of the test packet are selected from a set of attributes of normal packets normally sent between the secure and nonsecure computer networks. A defined test packet is validated against a set of filter rules in the firewall or matched against the filter rules to determine those filter rules with matching attributes to the defined packet. When validating, responsive to the failure of the test packet in the validating step, the filter rule in the set of filter rules that denied the test packet is displayed.

U.S. Pat. No. 6,052,788 (Wesinger, Jr., et al., Apr. 18, 2000), expressly incorporated herein by reference, relates to a firewall, providing enhanced network security and user transparency, for improved network security and maximum user convenience. The firewall employs "envoys" that exhibit the security robustness of prior-art proxies and the transparency and ease-of-use of prior-art packet filters, combining the best of both worlds. No traffic can pass through the firewall unless the firewall has established an envoy for that traffic. Both connection-oriented (e.g., TCP) and connectionless (e.g., UDP-based) services may be handled using envoys. Establishment of an envoy may be subjected to a myriad of tests to "qualify" the user, the requested communication, or both. Therefore, a high level of security may be achieved. The usual added burden of prior-art proxy systems is avoided in such a way as to achieve full transparency—the user can use standard applications and need not even know of the existence of the firewall. To achieve full transparency, the firewall is configured as two or more sets of virtual hosts. The firewall is, therefore, "multi-homed," each home being independently configurable. One set of hosts responds to addresses on a first network interface of the firewall. Another set of hosts responds to addresses on a second network interface of the firewall. In one aspect, programmable transparency is achieved by establishing DNS mappings between remote hosts to be accessed through one of the network interfaces and respective virtual hosts on that interface. In another aspect, automatic transparency may be achieved using code for dynamically mapping remote hosts to virtual hosts in accordance with a technique referred to herein as dynamic DNS, or DDNS.

U.S. Pat. No. 6,061,797 (Jade, et al., May 9, 2000), expressly incorporated herein by reference, relates to a system and method for providing outside access to computer resources through a firewall. A firewall isolates computer and network resources inside the firewall from networks, computers and computer applications outside the firewall. Typically, the inside resources could be privately owned databases and local area networks (LAN's), and outside objects could include individuals and computer applications operating through public communication networks such as the Internet. Usually, a firewall allows for an inside user or object to originate connection to an outside object or network, but does not allow for connections to be generated in the reverse direction; i.e. from outside in. The system provides a special tunneling mechanism, operating on both sides of a firewall, for establishing such "outside in" connections when they are requested by certain "trusted" individuals or objects or applications outside the firewall. The intent here is to minimize the resources required for establishing "tunneled" connections (connections through the firewall that are effectively requested from outside), while also minimizing the security risk involved in permitting such connections to be made at all. The mechanism includes special tunneling applications, running on interface servers inside and outside the firewall, and a special table of "trusted sockets" created and maintained by the inside tunneling application. Entries in the trusted sockets table define objects inside the firewall consisting of special inside ports, a telecommunication protocol to be used at each port, and a host object associated with each port. Each entry is "trusted" in the sense that it is supposedly known only by individuals authorized to have "tunneling" access through the firewall from outside.

U.S. Pat. No. 6,061,798 (Coley, et al., May 9, 2000), expressly incorporated herein by reference, relates to a firewall system for protecting network elements connected to a public network. The firewall operates on a stand-alone computer connected between the public network and the network elements to be protected such that all access to the protected network elements must go through the firewall. The firewall application running on the stand-alone computer is preferably the only application running on that machine. The application includes a variety of proxy agents that are specifically assigned to an incoming request in

accordance with the service protocol (i.e., port number) indicated in the incoming access request. An assigned proxy agent verifies the authority of an incoming request to access a network element indicated in the request. Once verified, the proxy agent completes the connection to the protected network element on behalf of the source of the incoming request.

See also, U.S. Pat. No. 6,075,860 (Apparatus and method for authentication and encryption of a remote terminal over a wireless link); U.S. Pat. No. 6,061,798 (Firewall system for protecting network elements connected to a public network); U.S. Pat. No. 6,061,797 (Outside access to computer resources through a firewall); U.S. Pat. No. 6,052,788 (Firewall providing enhanced network security and user transparency): U.S. Pat. No. 6,047,322 (Method and apparatus for quality of service management); U.S. Pat. No. 6,041,355 (Method for transferring data between a network of computers dynamically based on tag information); U.S. Pat. No. 6,012,088 (Automatic configuration for internet access device); U.S. Pat. No. 6,003,084 (Secure network proxy for connecting entities); U.S. Pat. No. 5,999,973 (Use of web technology for subscriber management activities); U.S. Pat. No. 5,991,731 (Method and system for interactive prescription and distribution of prescriptions in conducting clinical studies); U.S. Pat. No. 5,983,350 (Secure firewall supporting different levels of authentication based on address or encryption status); U.S. Pat. No. 5,968,176 (Multilayer firewall system); U.S. Pat. No. 5,960,177 (System for performing remote operation between firewall-equipped networks or devices); U.S. Pat. No. 5,958,016 (Internet-web link for access to intelligent network service control); U.S. Pat. No. 5,950,195 (Generalized security policy management system and method); U.S. Pat. No. 5,944,823 (Outside access to computer resources through a firewall); U.S. Pat. No. 5,928,333 (Electronic mail management system for operation on a host computer system); U.S. Pat. No. 5,918,227 (On-line directory service with a plurality of databases and processors); U.S. Pat. No. 5,915,087 (Transparent security proxy for unreliable message exchange protocols); U.S. Pat. No. 5,915,008 (System and method for changing advanced intelligent network services from customer premises equipment); U.S. Pat. No. 5,909,493 (Method and system for diagnosis and control of machines using connectionless modes of communication); U.S. Pat. No. 5,898,830 (Firewall providing enhanced network security and user transparency); U.S. Pat. No. 5,870,744 (Virtual people networking); U.S. Pat. No. 5,845,267 (System and method for billing for transactions conducted over the internet from within an intranet); U.S. Pat. No. 5,835,726 (System for securing the flow of and selectively modifying packets in a computer network); U.S. Pat. No. 5,826,029 (Secured gateway interface); U.S. Pat. No. 5,826,014 (Firewall system for protecting network elements connected to a public network); U.S. Pat. No. 5,812,398 (Method and system for escrowed backup of hotelled world wide web sites); U.S. Pat. No. 5,805,803 (Secure web tunnel); U.S. Pat. No. 5,784,463 (Token distribution, registration, and dynamic configuration of user entitlement for an application level security system and method); U.S. Pat. No. 5,632,011 (Electronic mail management system for operation on a host computer system); U.S. Pat. No. 5,623,601 (Apparatus and method for providing a secure gateway for communication and data exchanges between networks), U.S. Pat. No. 6,141,755 (Dowd, Firewall security apparatus for high speed circuit switched networks), each of which is expressly incorporated herein by reference.

Virtual Private Network

U.S. Pat. No. 6,079,020 (Liu, Jun. 20, 2000), expressly incorporated herein by reference, relates to a method and an apparatus for managing a virtual private network operating over a public data network. This public data network has been augmented to include a plurality of virtual private network gateways so that communications across the virtual private network are channeled through the virtual private network gateways. One embodiment includes a system that operates by receiving a command specifying an operation on the virtual private network. The system determines which virtual private network gateways are affected by the command. The system then automatically translates the command into configuration parameters for virtual private network gateways affected by the command. These configuration parameters specify how the virtual private network gateways handle communications between specific groups of addresses on the public data network. The system then transmits the configuration parameters to the virtual private network gateways affected by the command, so that the virtual private network gateways are configured to implement the command.

See also, U.S. Pat. No. 6,081,900 (Secure intranet access); U.S. Pat. No. 6,081,533 (Method and apparatus for an application interface module in a subscriber terminal unit); U.S. Pat. No. 6,079,020 (Method and apparatus for managing a virtual private network); U.S. Pat. No. 6,078,946 (System and method for management of connection oriented networks); U.S. Pat. No. 6,078,586 (ATM virtual private networks); U.S. Pat. No. 6,075,854 (Fully flexible routing service for an advanced intelligent network); U.S. Pat. No. 6,075,852 (Telecommunications system and method for processing call-independent signalling transactions); U.S. Pat. No. 6,073,172 (Initializing and reconfiguring a secure network interface); U.S. Pat. No. 6,061,796 (Multi-access virtual private network); U.S. Pat. No. 6,061,729 (Method and system for communicating service information in an advanced intelligent network); U.S. Pat. No. 6,058,303 (System and method for subscriber activity supervision); U.S. Pat. No. 6,055,575 (Virtual private network system and method); U.S. Pat. No. 6,052,788 (Firewall providing enhanced network security and user transparency); U.S. Pat. No. 6,047,325 (Network device for supporting construction of virtual local area networks on arbitrary local and wide area computer networks); U.S. Pat. No. 6,032,118 (Virtual private network service provider for asynchronous transfer mode network); U.S. Pat. No. 6,029,067 (Virtual private network for mobile subscribers); U.S. Pat. No. 6,016,318 (Virtual private network system over public mobile data network and virtual LAN); U.S. Pat. No. 6,009,430 (Method and system for provisioning databases in an advanced intelligent network); U.S. Pat. No. 6,005,859 (Proxy VAT-PSTN origination); U.S. Pat. No. 6,002,767 (System, method and article of manufacture for a modular gateway server architecture): U.S. Pat. No. 6,002,756 (Method and system for implementing intelligent telecommunication services utilizing self-sustaining, fault-tolerant object oriented architecture), each of which is expressly incorporated herein by reference.

Biometric Authentication

U.S. Pat. No. 5,193,855 (Shamos, Mar. 16, 1993, Patient and healthcare provider identification system), expressly incorporated herein by reference, relates to a patient and healthcare provider identification system which includes a database of patient and healthcare provider information including the identity of each patient and provider and some identification criteria (such as fingerprint data); a print

scanner for reading the print information from a patient or provider; a control system for matching the print data read by the scanner with the print data stored in memory; and a printer for printing labels or generating stamps or other visually perceptible medium for positively identifying the patient or provider and creating a record of the identification.

U.S. Pat. No. 6,035,406 (Moussa, et al., Mar. 7, 2000), expressly incorporated herein by reference, relates to a plurality-factor security system. The method and system provide for simultaneously authenticating a user using two or more factors, such as both a password and a physical token or both a password and biometric information. The user presents a physical token including a storage device to a processor and attempts to log in using a first password; the processor includes a login service which receives the first password, accesses the storage device to transform the first password into a second password, and authenticates the second password using an operating system for the processor. The storage device includes encrypted information regarding the second password which can be relatively easily determined in response to the first password, but which cannot be relatively easily determined without the first password. The system or the storage device may also store information for biometric authentication of the user.

U.S. Pat. No. 6,052,468 (Hillhouse, Apr. 18, 2000), expressly incorporated herein by reference, relates to a method is disclosed for improving portability of secure encryption key data files. The method provides for re-securing key data files according to different security processes for mobility. For porting an encryption key secured using a fingerprint authentication process to a system having only a password authentication process, a user selects password authentication process, provides a fingerprint and is authorized, provides a new password and then the encryption key is accessed according to the fingerprint authentication process and secured according to the password authentication process. This allows the use of specialized security hardware at one location while retaining an ability to transport encryption keys in a secure fashion to other locations, which do not have similar security hardware. U.S. Pat. No. 6,052,468 therefore provides a system and method for increasing portability of secure access codes, by providing a system comprising a cryptographic key encrypted and stored in a key data file and a secured key for decrypting the cryptographic key wherein the secured key is stored in a secured fashion, a method of securing the secured key comprising the steps of a) accessing stored data associated with the secured key, the data indicative of an access method from a plurality of access methods for accessing the secured key; b) executing the indicated access method to access the secured key; c) selecting a method from the plurality of methods for securing the accessed secured key; d) securing the accessed secured key according to the selected access method; and, e) storing data associated with the secured key, the data indicative of the selected access method. The key may be secured by providing user authentication information; deriving from the user authentication information a second cryptographic key; encrypting the accessed secured key using the second cryptographic key; and the secured key is accessed by the steps of: providing user authentication information; deriving from the user authentication information a third cryptographic key; and, decrypting the secured key using the third cryptographic key. A method of accessing a secured cryptographic key is provided comprising the steps of: a) accessing data associated with the secured cryptographic key to determine an authorization method necessary to access the secured cryptographic key; b) providing user authorization information; and c) executing the determined authorization method to access the secured cryptographic key based on the user authorization information provided. A further method is provided for securing portable key data including encryption key information comprising the steps of: a) selecting a first authorization process from a plurality of authorization processes for securing the portable key data; b) authenticating access to the secured portable key data according to a different authorization process, removing the security from the portable key data; and c) implementing security of the portable key data according to the first authorization process.

U.S. Pat. No. 6,076,167 (Borza, Jun. 13, 2000), expressly incorporated herein by reference, relates to a method of enhancing network security for a communication session initiated between a first computer and a second other computer. From the first computer to the second computer in communications therewith a process for securing communications therebetween is transmitted. One such process is a biometric characterization process for characterizing fingerprints. The process is for execution on the second computer and is selected to be compatible therewith. Communications from the second computer to the first computer are secured using the transmitted process on the second computer and using, on the first computer, a compatible process to the transmitted process. The host computer can modify or replace the process or data particular to the process before each session, during a session, or at intervals.

See also, U.S. Pat. No. 6,081,900 (Secure intranet access); U.S. Pat. No. 6,081,750 (Ergonomic man-machine interface incorporating adaptive pattern recognition based control system); U.S. Pat. No. 6,081,199 (Locking device for systems access to which is time-restricted); U.S. Pat. No. 6,079,621 (Secure card for E-commerce and identification); U.S. Pat. No. 6,078,265 (Fingerprint identification security system); U.S. Pat. No. 6,076,167 (Method and system for improving security in network applications); U.S. Pat. No. 6,075,455 (Biometric time and attendance system with epidermal topographical updating capability); U.S. Pat. No. 6,072,894 (Biometric face recognition for applicant screening); U.S. Pat. No. 6,070,141 (System and method of assessing the quality of an identification transaction using an identification quality score); U.S. Pat. No. 6,068,184 (Security card and system for use thereof); U.S. Pat. No. 6,064,751 (Document and signature data capture system and method); U.S. Pat. No. 6,056,197 (Information recording method for preventing alteration, information recording apparatus, and information recording medium); U.S. Pat. No. 6,052,468 (Method of securing a cryptographic key); U.S. Pat. No. 6,045,039 (Cardless automated teller transactions); U.S. Pat. No. 6,044,349 (Secure and convenient information storage and retrieval method and apparatus); U.S. Pat. No. 6,044,155 (Method and system for securely archiving core data secrets); U.S. Pat. No. 6,041,410 (Personal identification fob); U.S. Pat. No. 6,040,783 (System and method for remote, wireless positive identity verification); U.S. Pat. No. 6,038,666 (Remote identity verification technique using a personal identification device); U.S. Pat. No. 6,038,337 (Method and apparatus for object recognition); U.S. Pat. No. 6,038,315 (Method and system for normalizing biometric variations to authenticate users from a public database and that ensures individual biometric data privacy); U.S. Pat. No. 6,037,870 (Detector system for access control, and a detector assembly for implementing such a system); U.S. Pat. No. 6,035,406 (Plurality-factor security system); U.S. Pat. No. 6,035,402 (Virtual certificate authority); U.S. Pat. No. 6,035,398 (Cryptographic key

generation using biometric data); U.S. Pat. No. 6,031,910 (Method and system for the secure transmission and storage of protectable information); U.S. Pat. No. 6,026,166 (Digitally certifying a user identity and a computer system in combination); U.S. Pat. No. 6,018,739 (Biometric personnel identification system); U.S. Pat. No. 6,016,476 (Portable information and transaction processing system and method utilizing biometric authorization and digital certificate security); U.S. Pat. No. 6,012,049 (System for performing financial transactions using a smartcard); U.S. Pat. No. 6,012,039 (Tokenless biometric electronic rewards system); U.S. Pat. No. 6,011,858 (Memory card having a biometric template stored thereon and system for using same); U.S. Pat. No. 6,009,177 (Enhanced cryptographic system and method with key escrow feature); U.S. Pat. No. 6,006,328 (Computer software authentication, protection, and security system); U.S. Pat. No. 6,003,135 (Modular security device); U.S. Pat. No. 6,002,770 (Method for secure data transmission between remote stations); U.S. Pat. No. 5,999,637 (Individual identification apparatus for selectively recording a reference pattern based on a correlation with comparative patterns); U.S. Pat. No. 5,999,095 (Electronic security system); U.S. Pat. No. 5,995,630 (Biometric input with encryption); U.S. Pat. No. 5,991,431 (Mouse adapted to scan biometric data); U.S. Pat. No. 5,991,429 (Facial recognition system for security access and identification); U.S. Pat. No. 5,991,408 (Identification and security using biometric measurements); U.S. Pat. No. 5,987,155 (Biometric input device with peripheral port); U.S. Pat. No. 5,987,153 (Automated verification and prevention of spoofing for biometric data); U.S. Pat. No. 5,986,746 (Topographical object detection system); U.S. Pat. No. 5,984,366 (Unalterable self-verifying articles); U.S. Pat. No. 5,982,894 (System including separable protected components and associated methods); U.S. Pat. No. 5,979,773 (Dual smart card access control electronic data storage and retrieval system and methods); U.S. Pat. No. 5,978,494 (Method of selecting the best enroll image for personal identification); U.S. Pat. No. 5,974,146 (Real time bank-centric universal payment system); U.S. Pat. No. 5,970,143 (Remote-auditing of computer generated outcomes, authenticated billing and access control, and software metering system using cryptographic and other protocols); U.S. Pat. No. 5,966,446 (Time-bracketing infrastructure implementation); U.S. Pat. No. 5,963,908 (Secure logon to notebook or desktop computers); U.S. Pat. No. 5,963,657 (Economical skin-pattern-acquisition and analysis apparatus for access control; systems controlled thereby); U.S. Pat. No. 5,954,583 (Secure access control system); U.S. Pat. No. 5,952,641 (Security device for controlling the access to a personal computer or to a computer terminal); U.S. Pat. No. 5,951,055 (Security document containing encoded data block); U.S. Pat. No. 5,949,881 (Apparatus and method for cryptographic companion imprinting); U.S. Pat. No. 5,949,879 (Auditable security system for the generation of cryptographically protected digital data); U.S. Pat. No. 5,949,046 (Apparatus for issuing integrated circuit cards); U.S. Pat. No. 5,943,423 (Smart token system for secure electronic transactions and identification); U.S. Pat. No. 5,935,071 (Ultrasonic biometric imaging and identity verification system); U.S. Pat. No. 5,933,515 (User identification through sequential input of fingerprints); U.S. Pat. No. 5,933,498 (System for controlling access and distribution of digital property); U.S. Pat. No. 5,930,804 (Web-based biometric authentication system and method); U.S. Pat. No. 5,923,763 (Method and apparatus for secure document timestamping); U.S. Pat. No. 5,920,477 (Human factored interface incorporating adaptive pattern recognition based controller apparatus); U.S. Pat. No. 5,920,384 (Optical imaging device); U.S. Pat. No. 5,920,058 (Holographic labeling and reading machine for authentication and security applications); U.S. Pat. No. 5,915,973 (System for administration of remotely-proctored, secure examinations and methods therefor); U.S. Pat. No. 5,913,196 (System and method for establishing identity of a speaker); U.S. Pat. No. 5,913,025 (Method and apparatus for proxy authentication); U.S. Pat. No. 5,912,974 (Apparatus and method for authentication of printed documents); U.S. Pat. No. 5,912,818 (System for tracking and dispensing medical items); U.S. Pat. No. 5,910,988 (Remote image capture with centralized processing and storage); U.S. Pat. No. 5,907,149 (Identification card with delimited usage); U.S. Pat. No. 5,901,246 (Ergonomic man-machine interface incorporating adaptive pattern recognition based control system); U.S. Pat. No. 5,898,154 (System and method for updating security information in a time-based electronic monetary system); U.S. Pat. No. 5,897,616 (Apparatus and methods for speaker verification/identification/classification employing non-acoustic and/or acoustic models and databases); U.S. Pat. No. 5,892,902 (Intelligent token protected system with network authentication); U.S. Pat. No. 5,892,838 (Biometric recognition using a classification neural network); U.S. Pat. No. 5,892,824 (Signature capture/verification systems and methods); U.S. Pat. No. 5,890,152 (Personal feedback browser for obtaining media files); U.S. Pat. No. 5,889,474 (Method and apparatus for transmitting subject status information over a wireless communications network); U.S. Pat. No. 5,881,226 (Computer security system); U.S. Pat. No. 5,878,144 (Digital certificates containing multimedia data extensions); U.S. Pat. No. 5,876,926 (Method, apparatus and system for verification of human medical data); U.S. Pat. No. 5,875,108 (Ergonomic man-machine interface incorporating adaptive pattern recognition based control system); U.S. Pat. No. 5,872,849 (Enhanced cryptographic system and method with key escrow feature); U.S. Pat. No. 5,872,848 (Method and apparatus for witnessed authentication of electronic documents); U.S. Pat. No. 5,872,834 (Telephone with biometric sensing device); U.S. Pat. No. 5,870,723 (Tokenless biometric transaction authorization method and system); U.S. Pat. No. 5,869,822 (Automated fingerprint identification system); U.S. Pat. No. 5,867,802 (Biometrically secured control system for preventing the unauthorized use of a vehicle); U.S. Pat. No. 5,867,795 (Portable electronic device with transceiver and visual image display); U.S. Pat. No. 5,867,578 (Adaptive multi-step digital signature system and method of operation thereof); U.S. Pat. No. 5,862,260 (Methods for surveying dissemination of proprietary empirical data); U.S. Pat. No. 5,862,246 (Knuckle profile identity verification system); U.S. Pat. No. 5,862,723 (Method and apparatus for a cryptographically-assisted commercial network system designed to facilitate and support expert-based commerce); U.S. Pat. No. 5,857,022 (Enhanced cryptographic system and method with key escrow feature); U.S. Pat. No. 5,850,451 (Enhanced cryptographic system and method with key escrow feature); U.S. Pat. No. 5,850,442 (Secure world wide electronic commerce over an open network); U.S. Pat. No. 5,848,231) (System configuration contingent upon secure input); U.S. Pat. No. 5,844,244 (Portable identification carrier); U.S. Pat. No. 5,841,907 (Spatial integrating optical correlator for verifying the authenticity of a person, product or thing); U.S. Pat. No. 5,841,886 (Security system for photographic identification); U.S. Pat. No. 5,841,865 (Enhanced cryptographic system and method with key escrow feature); U.S. Pat. No. 5,841,122 (Security structure with electronic smart card access

thereto with transmission of power and data between the smart card and the smart card reader performed capacitively or inductively); U.S. Pat. No. 5,838,812 (Tokenless biometric transaction authorization system); U.S. Pat. No. 5,832,464 (System and method for efficiently processing payments via check and electronic funds transfer); U.S. Pat. No. 5,832,119 (Methods for controlling systems using, control signals embedded in empirical data); U.S. Pat. No. 5,828,751 (Method and apparatus for secure measurement certification); U.S. Pat. No. 5,825,880 (Multi-step digital signature method and system); U.S. Pat. No. 5,825,871 (Information storage device for storing personal identification information); U.S. Pat. No. 5,815,577 (Methods and apparatus for securely encrypting data in conjunction with a personal computer); U.S. Pat. No. 5,815,252 (Biometric identification process and system utilizing, multiple parameters scans for reduction of false negatives); U.S. Pat. No. 5,805,719 (Tokenless identification of individuals); U.S. Pat. No. 5,802,199 (Use sensitive identification system); U.S. Pat. No. 5,799,088 (Non-deterministic public key encryption system); U.S. Pat. No. 5,799,086 (Enhanced cryptographic system and method with key escrow feature); U.S. Pat. No. 5,799,083 (Event verification system); U.S. Pat. No. 5,790,674 (System and method of providing system integrity and positive audit capabilities to a positive identification system); U.S. Pat. No. 5,790,668 (Method and apparatus for securely handling data in a database of biometrics and associated data); U.S. Pat. No. 5,789,733 (Smart card with contactless optical interface); U.S. Pat. No. 5,787,187 (Systems and methods for biometric identification using the acoustic properties of the ear canal); U.S. Pat. No. 5,784,566 (System and method for negotiating security services and algorithms for communication across a computer network); U.S. Pat. No. 5,784,461 (Security system for controlling access to images and image related services); U.S. Pat. No. 5,774,551 (Pluggable account management interface with unified login and logout and multiple user authentication services); U.S. Pat. No. 5,771,071 (Apparatus for coupling multiple data sources onto a printed document); U.S. Pat. No. 5,770,849 (Smart card device with page an image display), U.S. Pat. No. 5,768,382 (Remote-auditing of computer generated outcomes and authenticated billing and access control system using cryptographic and other protocols); U.S. Pat. No. 5,767,496 (Apparatus for processing symbol-encoded credit card information); U.S. Pat. No. 5,764,789 (Tokenless biometric ATM access system); U.S. Pat. No. 5,763,862 (Dual card smart card reader); U.S. Pat. No. 5,761,298 (Communications headset with universally adaptable receiver and voice transmitter); U.S. Pat. No. 5,757,916 (Method and apparatus for authenticating the location of remote users of networked computing systems); U.S. Pat. No. 5,757,431 (Apparatus for coupling multiple data sources onto a printed document); U.S. Pat. No. 5,751,836 (Automated, non-invasive iris recognition system and method); U.S. Pat. No. 5,751,809 (Apparatus and method for securing captured data transmitted between two sources); U.S. Pat. No. 5,748,738 (System and method for electronic transmission, storage and retrieval of authenticated documents); U.S. Pat. No. 5,745,573 (System and method for controlling access to a user secret); U.S. Pat. No. 5,745,555 (System and method using personal identification numbers and associated prompts for controlling unauthorized use of a security device and unauthorized access to a resource); U.S. Pat. No. 5,742,685 (Method for verifying an identification card and recording verification of same); U.S. Pat. No. 5,742,683 (System and method for managing multiple users with different privileges in an open metering system); U.S. Pat. No. 5,737,420 (Method for secure data transmission between remote stations); U.S. Pat. No. 5,734,154 (Smart card with integrated reader and visual image display); U.S. Pat. No. 5,719,950 (Biometric, personal authentication system); U.S. Pat. No. 5,712,914 (Digital certificates containing multimedia data extensions); U.S. Pat. No. 5,712,912 (Method and apparatus for securely handling a personal identification number or cryptographic key using biometric techniques); U.S. Pat. No. 5,706,427 (Authentication method for networks); U.S. Pat. No. 5,703,562 (Method for transferring data from an unsecured computer to a secured computer); U.S. Pat. No. 5,696,827 (Secure cryptographic methods for electronic transfer of information); U.S. Pat. No. 5,682,142 (Electronic control system/network); U.S. Pat. No. 5,682,032 (Capacitively coupled identity verification and escort memory apparatus); U.S. Pat. No. 5,680,460 (Biometric controlled key generation); U.S. Pat. No. 5,668,878 (Secure cryptographic methods for electronic transfer of information); U.S. Pat. No. 5,666,400 (Intelligent recognition); U.S. Pat. No. 5,659,616 (Method for securely using digital signatures in a commercial cryptographic system); U.S. Pat. No. 5,647,364 (Ultrasonic biometric imaging and identity verification system); U.S. Pat. No. 5,647,017 (Method and system for the verification of handwritten signatures); U.S. Pat. No. 5,646,839 (Telephone-based personnel tracking system); U.S. Pat. No. 5,636,282 (Method for dial-in access security using a multimedia modem); U.S. Pat. No. 5,633,932 (Apparatus and method for preventing disclosure through user-authentication at a printing node); U.S. Pat. No. 5,615,277 (Tokenless security system for authorizing access to a secured computer system); U.S. Pat. No. 5,613,012 (Tokenless identification system for authorization of electronic transactions and electronic transmissions); U.S. Pat. No. 5,608,387 (Personal identification devices and access control systems); U.S. Pat. No. 5,594,806 (Knuckle profile identity verification system); U.S. Pat. No. 5,592,408 (Identification card and access control device); U.S. Pat. No. 5,588,059 (Computer system and method for secure remote communication sessions); U.S. Pat. No. 5,586,171 (Selection of a voice recognition data base responsive to video data); U.S. Pat. No. 5,583,950 (Method and apparatus for flash correlation); U.S. Pat. No. 5,583,933 (Method and apparatus for the secure communication of data); U.S. Pat. No. 5,578,808 (Data card that can be used for transactions involving separate card issuers); U.S. Pat. No. 5,572,596 (Automated, non-invasive iris recognition system and method); U.S. Pat. No. 5,561,718 (Classifying faces); U.S. Pat. No. 5,559,885 (Two stage read-write method for transaction cards); U.S. Pat. No. 5,557,765 (System and method for data recovery); U.S. Pat. No. 5,553,155 (Low cost method employing time slots for thwarting fraud in the periodic issuance of food stamps, unemployment benefits or other governmental human services); U.S. Pat. No. 5,544,255 (Method and system for the capture, storage, transport and authentication of handwritten signatures); U.S. Pat. No. 5,534,855 (Method and system for certificate based alias detection); U.S. Pat. No. 5,533,123 (Programmable distributed personal security); U.S. Pat. No. 5,526,428 (Access control apparatus and method); U.S. Pat. No. 5,523,739 (Metal detector for control of access combined in an integrated form with a transponder detector); U.S. Pat. No. 5,497,430 (Method and apparatus for image recognition using invariant feature signals); U.S. Pat. No. 5,485,519 (Enhanced security for a secure token code); U.S. Pat. No. 5,485,312 (Optical pattern recognition system and method for verifying the authenticity of a person, product or thing); U.S. Pat. No. 5,483,601 (Apparatus and method for

biometric identification using silhouette and displacement images of a portion of a person's hand); U.S. Pat. No. 5,478,993 (Process as safety concept against unauthorized use of a payment instrument in cashless payment at payment sites); U.S. Pat. No. 5,475,839 (Method and structure for securing access to a computer system); U.S. Pat. No. 5,469,506 (Apparatus for verifying an identification card and identifying a person by means of a biometric characteristic); U.S. Pat. No. 5,457,747 (Anti-fraud verification system using a data card); U.S. Pat. No. 5,455,407 (Electronic-monetary system); U.S. Pat. No. 5,453,601 (Electronic-monetary system); U.S. Pat. No. 5,448,045 (System for protecting computers via intelligent tokens or smart cards); U.S. Pat. No. 5,432,864 (Identification card verification system); U.S. Pat. No. 5,414,755 (System and method for passive voice verification in a telephone network); U.S. Pat. No. 5,412,727 (Anti-fraud voter registration and voting system using a data card); U.S. Pat. No. 5,363,453 (Non-minutiae automatic fingerprint identification system and methods); U.S. Pat. No. 5,347,580 (Authentication method and system with a smartcard); U.S. Pat. No. 5,345,549 (Multimedia based security systems); U.S. Pat. No. 5,341,428 (Multiple cross-check document verification system); U.S. Pat. No. 5,335,288 (Apparatus and method for biometric identification); U.S. Pat. No. 5,291,560 (Biometric personal identification system based on iris analysis); U.S. Pat. No. 5,283,431 (Optical key security access system); U.S. Pat. No. 5,280,527 (Biometric token for authorizing access to a host system); U.S. Pat. No. 5,272,754 (Secure computer interface); U.S. Pat. No. 5,245,329 (Access control system with mechanical keys which store data); U.S. Pat. No. 5,229,764 (Continuous biometric authentication matrix); U.S. Pat. No. 5,228,094 (Process of identifying and authenticating data characterizing an individual); U.S. Pat. No. 5,224,173 (Method of reducing fraud in connection with employment, public license applications, social security, food stamps, welfare or other government benefits); U.S. Pat. No. 5,208,858 (Method for allocating useful data to a specific originator); U.S. Pat. No. 5,204,670 (Adaptable electric monitoring and identification system); U.S. Pat. No. 5,191,611 (Method and apparatus for protecting material on storage media and for transferring material on storage media to various recipients); U.S. Pat. No. 5,163,094 (Method for identifying individuals from analysis of elemental shapes derived from biosensor data); U.S. Pat. No. 5,155,680 (Billing system for computing software); U.S. Pat. No. 5,131,038 (Portable authentification system); U.S. Pat. No. 5,073,950 (Finger profile identification system); U.S. Pat. No. 5,067,162 (Method and apparatus for verifying identity using image correlation); U.S. Pat. No. 5,065,429 (Method and apparatus for protecting material on storage media); U.S. Pat. No. 5,056,147 (Recognition procedure and an apparatus for carrying out the recognition procedure); U.S. Pat. No. 5,056,141 (Method and apparatus for the identification of personnel); U.S. Pat. No. 5,036,461 (Two-way authentication system between user's smart card and issuer-specific plug-in application modules in multi-issued transaction device); U.S. Pat. No. 5,020,105 (Field initialized authentication system for protective security of electronic information networks); U.S. Pat. No. 4,993,068 (Unforgettable personal identification system); U.S. Pat. No. 4,972,476 (Counterfeit proof ID card having a scrambled facial image); U.S. Pat. No. 4,961,142 (Multi-issuer transaction device with individual identification verification plug-in application modules for each issuer); U.S. Pat. No. 4,952,928 (Adaptable electronic monitoring and identification system); U.S. Pat. No. 4,941,173 (Device and method to render secure the transfer of data between a videotex terminal and a server); U.S. Pat. No. 4,926,480 (Card-computer moderated systems); U.S. Pat. No. 4,896,363 (Apparatus and method for matching image characteristics such as fingerprint minutiae); U.S. Pat. No. 4,890,323 (Data communication systems and methods); U.S. Pat. No. 4,868,376 (Intelligent portable interactive personal data system); U.S. Pat. No. 4,827,518 (Speaker verification system using integrated circuit cards); U.S. Pat. No. 4,819,267 (Solid state key for controlling access to computer systems and to computer software and/or for secure communications); U.S. Pat. No. 4,752,676 (Reliable secure, updatable "cash" card system); U.S. Pat. No. 4,736,203 (3D hand profile identification apparatus); U.S. Pat. No. 4,731,841 (Field initialized authentication system for protective security of electronic information networks); U.S. Pat. No. 4,564,018 (Ultrasonic system for obtaining ocular measurements), each of which is expressly incorporated herein by reference.

Content-Based Query Servers

U.S. Pat. No. 5,987,459 (Swanson, et al. Nov. 16, 1999), expressly incorporated herein by reference, relates to an image and document management system for content-based retrieval support directly into the compressed files. The system minimizes a weighted sum of the expected size of the compressed files and the expected query response time. Object searching of documents stored by the system is possible on a scalable resolution basis. The system includes a novel object representation based on embedded prototypes that provides for high-quality browsing of retrieval images at low bit rates.

U.S. Pat. No. 6,038,560 (Wical, Mar. 14, 2000), expressly incorporated herein by reference, relates to a concept knowledge base search and retrieval system, which includes factual knowledge base queries and concept knowledge base queries, is disclosed. A knowledge base stores associations among terminology/categories that have a lexical, semantic or usage association. Document theme vectors identify the content of documents through themes as well as through classification of the documents in categories that reflects what the documents are primarily about. The factual knowledge base queries identify, in response to an input query, documents relevant to the input query through expansion of the query terms as well as through expansion of themes. The concept knowledge base query does not identify specific documents in response to a query, but specifies terminology that identifies the potential existence of documents in a particular area.

U.S. Pat. No. 6,067,466 (Selker, et al., May 23, 2000), expressly incorporated herein by reference, relates to a diagnostic tool using a predictive instrument. A method is provided for evaluating a medical condition of a patient including the steps of monitoring one or more clinical features of a patient; based on the monitored features, computing a primary probability of a medical outcome or diagnosis; computing a plurality of conditional probabilities for a selected diagnostic test, the computed conditional probabilities including a first probability of the medical outcome or diagnosis assuming the selected diagnostic test produces a first outcome and a second probability of the medical outcome or diagnosis assuming the selected diagnostic test produces a second outcome; and displaying the computed primary probability as well as the plurality of computed conditional probabilities to a user as an aid to determining whether to administer the selected diagnostic test to the patient.

E-Commerce Systems

U.S. Pat. No. 5,946,669 (Polk, Aug. 31, 1999), expressly incorporated herein by reference, relates to a method and apparatus for payment processing using debit-based electronic funds transfer and disbursement processing using addendum-based electronic data interchange. This disclosure describes a payment and disbursement system, wherein an initiator authorizes a payment and disbursement to a collector and the collector processes the payment and disbursement through an accumulator agency. The accumulator agency processes the payment as a debit-based transaction and processes the disbursement as an addendum-based transaction. The processing of a debit-based transaction generally occurs by electronic funds transfer (EFT) or by financial electronic data interchange (FEDI). The processing of an addendum-based transaction generally occurs by electronic data interchange (EDI).

U.S. Pat. No. 6,005,939 (Fortenberry, et al., Dec. 21, 1999), expressly incorporated herein by reference, relates to a method and apparatus for storing an Internet user's identity and access rights to World Wide Web resources. A method and apparatus for obtaining user information to conduct secure transactions on the Internet without having to re-enter the information multiple times is described. The method and apparatus can also provide a technique by which secured access to the data can be achieved over the Internet. A passport containing user-defined information at various security levels is stored in a secure server apparatus, or passport agent, connected to computer network. A user process instructs the passport agent to release all or portions of the passport to a recipient node and forwards a key to the recipient node to unlock the passport information.

U.S. Pat. No. 6,016,484 (Williams, et al., Jan. 18, 2000), expressly incorporated herein by reference, relates to a system, method and apparatus for network electronic payment instrument and certification of payment and credit collection utilizing a payment. An electronic monetary system provides for transactions utilizing an electronic-monetary system that emulates a wallet or a purse that is customarily used for keeping money, credit cards and other forms of payment organized. Access to the instruments in the wallet or purse is restricted by a password to avoid unauthorized payments. A certificate form must be completed in order to obtain an instrument. The certificate form obtains the information necessary for creating a certificate granting authority to utilize an instrument, a payment holder and a complete electronic wallet. Electronic approval results in the generation of an electronic transaction to complete the order. If a user selects a particular certificate, a particular payment instrument holder will be generated based on the selected certificate. In addition, the issuing agent for the certificate defines a default bitmap for the instrument associated with a particular certificate, and the default bitmap will be displayed when the certificate definition is completed. Finally, the number associated with a particular certificate will be utilized to determine if a particular party can issue a certificate.

U.S. Pat. No. 6,029,150 (Kravitz, Feb. 22, 2000), expressly incorporated herein by reference, relates to a system and method of payment in an electronic payment system wherein a plurality of customers have accounts with an agent. A customer obtains an authenticated quote from a specific merchant, the quote including a specification of goods and a payment amount for those goods. The customer sends to the agent a single communication including a request for payment of the payment amount to the specific merchant and a unique identification of the customer. The agent issues to the customer an authenticated payment advice based only on the single communication and secret shared between the customer and the agent and status information, which the agent knows about the merchant, and/or the customer. The customer forwards a portion of the payment advice to the specific merchant. The specific merchant provides the goods to the customer in response to receiving the portion of the payment advice.

U.S. Pat. No. 6,047,269 (Biffar, Apr. 4, 2000), expressly incorporated herein by reference, relates to a self-contained payment system with creating and facilitating transfer of circulating digital vouchers representing value. A digital voucher has an identifying element and a dynamic log. The identifying element includes information such as the transferable value, a serial number and a digital signature. The dynamic log records the movement of the voucher through the system and accordingly grows over time. This allows the system operator to not only reconcile the vouchers before redeeming them, but also to recreate the history of movement of a voucher should an irregularity like a duplicate voucher be detected. These vouchers are used within a self-contained system including a large number of remote devices that are linked to a central system. The central system can e linked to an external system. The external system, as well as the remote devices, is connected to the central system by any one or a combination of networks. The networks must be able to transport digital information, for example the Internet, cellular networks, telecommunication networks, cable networks or proprietary networks. Vouchers can also be transferred from one remote device to another remote device. These remote devices can communicate through a number of methods with each other. For example, for a non-face-to-face transaction the Internet is a choice, for a face-to-face or close proximity transactions tone signals or light signals are likely methods. In addition, at the time of a transaction a digital receipt can be created which will facilitate a fast replacement of vouchers stored in a lost remote device.

See, U.S. Pat. No. 6,134,328 (Cordery, Secure User Certification for Electronic Commerce Employing Value Metering System), and U.S. Pat. No. 5,796,841 (Cordery, Secure User Certification for Electronic Commerce Employing Value Metering System); U.S. Pat. No. 6,148,338 (Lachelt, System for Logging and Enabling Ordered Retrieval of Management), expressly incorporated herein by reference.

A. Michael Froomkin, The Essential Role of Trusted Third Parties in Electronic Commerce, 75 Oregoon Law Review 49–115 (1996).

Oscar H. Gandy, Jr., Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace, 1996 University of Chicago Law Forum 77–91 (1996).

Trotter Hardy, Property and (Copyright) in Cyberspace 1996 University of Chicago Law Forum 217–260 (1996).

Vicky E. Jones, N. Ching, & M. Winslett, Credentials for Privacy and Interoperation: . . . New Security Paradigms, '95 Workshop, LaJolla, Cal. Aug. 22–25, 1995.

Peter Keen, Craigg Ballance, Sally Chan, and Steve Schrump, Electronic Relationships: Trust by Design (2000).

George Lawton, The Internets Challenge to Privacy, IEEE Computer, Vol. 31, No. 6, June 1998. pp. 16–18.

Lawrence Lessig, The Path of Cyberlaw, 104 Yale Law Journal 1743–1755 (1995).

Hiroshi Maruyama and Takeshi Imamura, Element-Wise XML Encryption, http://www.trl.ibm.com/projects/xml/xss4j/docs/ewe-paper.html.

Shamkant B. Navathe and Michael J. Donahoo, Towards Intelligent Integration of Heterogenous Information Sources, Proceedings of the 6th International Workshop on Database Reengineering and Interoperability, March 1995.

Leon Pintsov and Scott Vanstone, Postal Revenue Collection in the Digital Age, Proc. of Financial Cryptography '00, Feb. 22, 2000.

Pamela Samuelson, Liability for Defective Information, Communications of the ACM, Vol. 36, No. 5, May 1993, pp. 21–26.

United States Senate Judiciary Committee, Know the Rules; Use the Tools; Privacy in the Digital Age at http://judiciary.senate.gov/privacy.htm.

Gio Wiederhold, Trends for the Information Technology Industry, http://www-db.stanford.edu/pub/gio/1999/miti.htm.

Gio Wiederhold, Value Added Middleware: Mediators at http://www-db.stanford.edu/pub/gio/1998/dbpd.html.

Micropayments

U.S. Pat. No. 5,999,919 (Jarecki, et al., Dec. 7, 1999), expressly incorporated herein by reference, relates to an efficient micropayment system. Existing software proposals for electronic payments can be divided into "on-line" schemes which require participation of a trusted party (the bank) in every transaction and are secure against overspending, and "off-line" schemes which do not require a third party and guarantee only that overspending is detected when vendors submit their transaction records to the bank (usually at the end of the day). A new "hybrid" scheme is proposed which combines the advantages of both "on-line" and "off-line" electronic payment schemes. It allows for control of overspending at a cost of only a modest increase in communication compared to the off-line schemes. The protocol is based on probabilistic polling. During each transaction, with some small probability, the vendor forwards information about this transaction to the bank. This enables the bank to maintain an accurate approximation of a customer's spending. The frequency of polling messages is related to the monetary value of transactions and the amount of overspending the bank is willing to risk. For transactions of high monetary value, the cost of polling approaches that of the on-line schemes, but for micropayments, the cost of polling is a small increase over the traffic incurred by the off-line schemes.

Micropayments are often preferred where the amount of the transaction does not justify the costs of complete financial security. In the micropayment scheme, typically a direct communication between creditor and debtor is not required; rather, the transaction produces a result which eventually results in an economic transfer, but which may remain outstanding subsequent to transfer of the underlying goods or services. The theory underlying this micropayment scheme is that the monetary units are small enough such that risks of failure in transaction closure is relatively insignificant for both parties, but that a user gets few chances to default before credit is withdrawn. On the other hand, the transaction costs of a non-real time transactions of small monetary units are substantially less than those of secure, unlimited or potentially high value, real time verified transactions, allowing and facilitating such types of commerce. Thus, the rights management system may employ applets local to the client system, which communicate with other applets and/or the server and/or a vendor/rights-holder to validate a transaction, at low transactional costs.

The following U.S. patents, expressly incorporated herein by reference, define aspects of micropayment, digital certificate, and on-line payment systems: U.S. Pat. No. 5,930,777 (Barber, Jul. 27, 1999, Method of charging for pay-per-access information over a network); U.S. Pat. No. 5,857,023 (Jan. 5, 1999, Demers et al., Space efficient method of redeeming electronic payments); U.S. Pat. No. 5,815,657 (Sep. 29, 1998, Williams, System, method and article of manufacture for network electronic authorization utilizing an authorization instrument); U.S. Pat. No. 5,793,868 (Aug. 11, 1998, Micali, Certificate revocation system), U.S. Pat. No. 5,717,757 (Feb. 10, 1998, Micali, Certificate issue lists); U.S. Pat. No. 5,666,416 (Sep. 9, 1997, Micali, Certificate revocation system); U.S. Pat. No. 5,677,955 (Doggett et al., Electronic funds transfer instruments); U.S. Pat. No. 5,839,119 (Nov. 17, 1998, Krsul; et al., Method of electronic payments that prevents double-spending); U.S. Pat. No. 5,915,093 (Berlin et al.); U.S. Pat. No. 5,937,394 (Wong, et al.); U.S. Pat. No. 5,933,498 (Schneck et al.); U.S. Pat. No. 5,903,880 (Biffar); U.S. Pat. No. 5,903,651 (Kocher); U.S. Pat. No. 5,884,277 (Khosla); U.S. Pat. No. 5,960,083 (Sep. 28, 1999, Micali, Certificate revocation system); U.S. Pat. No. 5,963,924 (Oct. 5, 1999, Williams et al., System, method and article of manufacture for the use of payment instrument holders and payment instruments in network electronic commerce); U.S. Pat. No. 5,996,076 (Rowney et al., System, method and article of manufacture for secure digital certification of electronic commerce); U.S. Pat. No. 6,016,484 (Jan. 18, 2000, Williams et al., System, method and article of manufacture for network electronic payment instrument and certification of payment and credit collection utilizing a payment); U.S. Pat. No. 6,018,724 (Arent); U.S. Pat. No. 6,021,202 (Anderson et al., Method and system for processing electronic documents); U.S. Pat. No. 6,035,402 (Vaeth et al.); U.S. Pat. No. 6,049,786 (Smorodinsky); U.S. Pat. No. 6,049,787 (Takahashi, et al.); U.S. Pat. No. 6,058,381 (Nelson, Many-to-many payments system for network content materials); U.S. Pat. No. 6,061,448 (Smith, et al.); U.S. Pat. No. 5,987,132 (Nov. 16, 1999, Rowney, System, method and article of manufacture for conditionally accepting a payment method utilizing an extensible, flexible architecture); U.S. Pat. No. 6,057,872 (Candelore); and U.S. Pat. No. 6,061,665 (May 9, 2000, Bahreman, System, method and article of manufacture for dynamic negotiation of a network payment framework). See also, Rivest and Shamir, "PayWord and MicroMint: Two Simple Micropayment Schemes" (May 7, 1996); Micro PAYMENT transfer Protocol (MPTP) Version 0.1 (22 Nov. 95) et seq., http://www.w3.org/pub/WWW/TR/WD-mptp; Common Markup for web Micropayment Systems, http://www.w3.org/TR/WD-Micropayment-Markup (09 Jun. 99); "Distributing Intellectual Property: a Model of Microtransaction Based Upon Metadata and Digital Signatures", Olivia, Maurizio, http://olivia.modlang.denison.edu/~olivia/RFC/09/, all of which are expressly incorporated herein by reference.

See, also: U.S. Pat. No. 4,977,595 (Dec. 11, 1990, Method and apparatus for implementing electronic cash); U.S. Pat. No. 5,224,162 (Jun. 29, 1993, Electronic cash system); U.S. Pat. No. 5,237,159 (Aug. 17, 1993, Electronic check presentment system); U.S. Pat. No. 5,392,353 (2/1995, Morales, TV Answer, Inc. Interactive satellite broadcast network); U.S. Pat. No. 5,511,121 (Apr. 23, 1996, Efficient electronic money); U.S. Pat. No. 5,621,201 (4/1997, Langhans et al., Visa International Automated purchasing control system); U.S. Pat. No. 5,623,547 (Apr. 22, 1997, Value transfer system); U.S. Pat. No. 5,679,940 (10/1997, Templeton et al., TeleCheck International, Inc. Transaction system with on/off line risk assessment); U.S. Pat. No. 5,696,908 (12/1997, Muehlberger et al., Southeast Phonecard, Inc.

Telephone debit card dispenser and method); U.S. Pat. No. 5,754,939 (5/1998, Herz et al., System for generation of user profiles for a system for customized electronic identification of desirable objects); U.S. Pat. No. 5,768,385 (Jun. 16, 1998, Untraceable electronic cash); U.S. Pat. No. 5,799,087 (Aug. 25, 1998, Electronic-monetary system); U.S. Pat. No. 5,812,668 (Sep. 22, 1998, System, method and article of manufacture for verifying the operation of a remote transaction clearance system utilizing a multichannel, extensible, flexible architecture); U.S. Pat. No. 5,828,840 (Oct. 27, 1998, Server for starting client application on client if client is network terminal and initiating client application on server if client is non network terminal); U.S. Pat. No. 5,832,089 (Nov. 3, 1998, Off-line compatible electronic cash method and system); U.S. Pat. No. 5,850,446 (Dec. 15, 1998, System, method and article of manufacture for virtual point of sale processing utilizing an extensible, flexible architecture); U.S. Pat. No. 5,889,862 (Mar. 30, 1999, Method and apparatus for implementing traceable electronic cash); U.S. Pat. No. 5,889,863 (Mar. 30, 1999, System, method and article of manufacture for remote virtual point of sale processing utilizing a multichannel, extensible, flexible architecture); U.S. Pat. No. 5,898,154 (Apr. 27, 1999, System and method for updating security information in a time-based electronic monetary system); U.S. Pat. No. 5,901,229 (May 4, 1999, Electronic cash implementing method using a trustee); U.S. Pat. No. 5,920,629 (Jul. 6, 1999, Electronic-monetary system); U.S. Pat. No. 5,926,548 (Jul. 20, 1999, Method and apparatus for implementing hierarchical electronic cash); U.S. Pat. No. 5,943,424 (Aug. 24, 1999, System, method and article of manufacture for processing a plurality of transactions from a single initiation point on a multichannel, extensible, flexible architecture); U.S. Pat. No. 5,949,045 (Sep. 7, 1999, Micro-dynamic simulation of electronic cash transactions); U.S. Pat. No. 5,952,638 (Sep. 14, 1999, Space efficient method of electronic payments); U.S. Pat. No. 5,963,648 (Oct. 5, 1999, Electronic-monetary system); U.S. Pat. No. 5,978,840 (System, method and article of manufacture for a payment gateway system architecture for processing encrypted payment transactions utilizing a multichannel, extensible, flexible architecture); U.S. Pat. No. 5,983,208 (Nov. 9, 1999, System, method and article of manufacture for handling transaction results in a gateway payment architecture utilizing a multichannel, extensible, flexible architecture); U.S. Pat. No. 5,987,140 (Nov. 16, 1999, System, method and article of manufacture for secure network electronic payment and credit collection); U.S. Pat. No. 6,002,767 (Dec. 14, 1999, System, method and article of manufacture for a modular gateway server architecture); U.S. Pat. No. 6,003,765 (Dec. 12, 1999, Electronic cash implementing method with a surveillance institution, and user apparatus and surveillance institution apparatus for implementing the same); U.S. Pat. No. 6,021,399 (Feb. 1, 2000, Space efficient method of verifying electronic payments); U.S. Pat. No. 6,026,379 (Feb. 15, 2000, System, method and article of manufacture for managing transactions in a high availability system); U.S. Pat. No. 6,029,150 (Feb. 22, 2000, Payment and transactions in electronic commerce system); U.S. Pat. No. 6,029,151 (Feb. 22, 2000, Method and system for performing electronic money transactions); U.S. Pat. No. 6,047,067 (Apr. 4, 2000, Electronic-monetary system); U.S. Pat. No. 6,047,887 (Apr. 11, 2000, System and method for connecting money modules); U.S. Pat. No. 6,055,508 (Apr. 25, 2000, Method for secure accounting and auditing on a communications network); U.S. Pat. No. 6,065,675 (May 23, 2000, Processing system and method for a heterogeneous electronic cash environment); U.S. Pat. No. 6,072,870 (Jun. 6, 2000, System, method and article of manufacture for a gateway payment architecture utilizing a multichannel, extensible, flexible architecture), each of which is expressly incorporated herein by reference.

Memory Cards

U.S. Pat. No. 6,021,393 (Honda, et al., Feb. 1, 2000), expressly incorporated herein by reference, relates to a medical information management system. As a portable memory card carried by a patient to store the patient's personal medical information, a hybrid-type memory card is used which includes an optical information recording area, an integrated circuit memory area and a magnetic information recording area. A read/write drive for the memory card includes an optical head, a carrier mechanism for loading the memory card on a carrier table and moving the loaded memory card relative to the optical head, and a coupler section for coupling electronic information to be read and written from and to the integrated circuit memory area of the memory card, so that reading and writing of optical information from and to the optical information recording area can be conducted simultaneously with reading and writing of the electronic information from and to the integrated circuit memory area.

U.S. Pat. No. 6,031,910 (Deindl, et al., Feb. 29, 2000), expressly incorporated herein by reference, relates to a method and system for the secure transmission and storage of protectable information, such as patient information, by means of a patient card. The data stored on the patient card are protected by cryptographic methods. The data is decrypted only with the same patient card if a doctor is authorized and the patient has given his agreement. AU information that the patient card needs in order to decide whether the doctor is authorized, and the key for protecting the control data and the random key are held on the chip. The patient data can be freely transmitted to any storage medium. The chip controls both the access to the data and the encryption and decryption functions. Random keys, which are themselves stored encrypted together with the data, ensure that every data record remains separate from every other data record, and that only authorized persons can access it. Every patient card has its own record key. The system and method are not directed exclusively to patient data but can be applied to any protectable data to which right of access is to be restricted.

U.S. Pat. No. 6,034,605 (March, Mar. 7, 2000), expressly incorporated herein by reference, relates to a system and method for secure storage of personal information and for broadcast of the personal information at a time of emergency. A sealed package contains a medium storing personal information associated with an individual. The sealed package is stored at a facility until an emergency occurs. At a time of emergency, a missing person report concerning the individual generated by a law enforcement agency is processed. The personal information in the individual's sealed package is accessed in response to the missing person report and then broadcast on an electronic bulletin board accessible via the Internet.

U.S. Pat. No. 6,042,005 (Basile, et al., Mar. 28, 2000), expressly incorporated herein by reference, relates to a personal identification system for children, that includes two forms of identification. An identification card carried by the user contains the user's personal and medical information in an electronic medium. The identification card includes photographs of the user and their parent or legal guardian, a unique identification number for the user, and a list of corporate sponsors. The second identification device is to be

worn by the user and includes the user's unique identification number and an access telephone number. A user interface enables the users to update their stored personal and medical information.

Jurisdictional Processing Dependence

U.S. Pat. No. 6,064,968 (Schanz, May 16, 2000), expressly incorporated herein by reference, relates to systems, methods and computer program products for identifying unique and common legal requirements for a regulated activity among multiple legal jurisdictions. Systems, methods and computer program products facilitate user compliance with laws that pertain to a regulated activity in each of a plurality of legal jurisdictions. A user selects, via a user interface in communication with a data processing system, a component that relates to an aspect of the regulated activity. A user also selects, via a user interface in communication with the data processing system, first and second legal jurisdictions from the plurality of legal jurisdictions. In response to the user selections, elements of the selected component that are unique and common to the first and second legal jurisdictions are displayed. Each displayed element is a legal requirement associated with the regulated activity as defined by laws of a respective legal jurisdiction.

What is claimed is:

1. A method for processing information, comprising the steps of:

receiving information to be processed:

defining a cryptographic comprehension function for the information, adapted for making at least a portion of the information incomprehensible;

receiving asymmetric cryptographic key information, comprising at least asymmetric encryption key information and asymmetric decryption key information;

negotiating a new cryptographic comprehension function between two parties to a communication using an intermediary;

processing the information to invert the cryptographic comprehension function and impose the new cryptographic comprehension function in an integral process, in dependence on at least the asymmetric cryptographic key information, without providing the intermediary with sufficient asymmetric cryptographic key information to decrypt the processed information; and

outputting processed information,

wherein the ability of the asymmetric decryption key information to decrypt the processed information changes dynamically.

2. The method according to claim **1**, further comprising the step of accounting for a decryption of the processed information.

3. The method according to claim **1**, wherein the ability of the asymmetric decryption key information to decrypt the processed information changes over time.

4. The method according to claim **1**, wherein said new cryptographic comprehension function has a cryptographic security based on an asymmetry between a difficulty of exponentiation of a message with a number derived from at least two large prime numbers, and a factoring thereof.

5. The method according to claim **1**, wherein said integral process comprises exponentiation of a message with a cryptographic key derived from at least two pairs of large primes.

6. The method according to claim **1**, wherein said cryptographic comprehension function comprises an exponentiation of a message or a cryptographic key with a key derived from at least two large prime numbers, and said integral process comprises exponentiation of a message or a cryptographic key with a number derived by combining a complementary key with an additional key derived from at least two large primes.

7. The method according to claim **1**, wherein said cryptographic comprehension function comprises a first RSA-type asymmetric key encryption, and said integral process comprises applying a second RSA-type asymmetric key encryption using an encryption key formed by multiplying a decryption key for said first RSA-type asymmetric key encryption with an encryption key for a second RSA-type asymmetric key encryption.

8. The method according to claim **1**, wherein the received information comprises AES cryptographic key information, and said comprehension function comprises an RSA type encryption algorithm employing a composite key defined by a function of a public key and a private key.

9. The method according to claim **8**, wherein the sender authenticates himself and enters into a non-repudiatable transaction with a third party to obtain at least one of the required keys by signing a message with the sender private key.

10. The method according to claim **1**, wherein:

said defining step comprises providing information encrypted with a large prime-number based asymmetric key encryption algorithm encrypted with a first key; and

said processing step comprises processing the provided information with a modified large prime-number based asymmetric key encryption algorithm using a composite key comprising a function of an complementary key to said first key and a second key.

11. The method according to claim **1**, wherein at least one party to a communication of the processed information authenticates himself and enters into a non-repudiatable transaction with a third party to obtain at least a portion of the asymmetric cryptographic key information by signing a message with a respective party private key.

12. The method according to claim **1**, wherein said processing step is performed in a secure environment protected from a sender of the information.

13. The method according to claim **1**, further comprising the steps of:

(a) defining first and second key pairs, having a compatible modulus; and

(b) said processing step comprises exponentiating a message encrypted with the cryptographic comprehension function using a first key of the first key pair, with a product of a second key of the first key pair and a first key of the second key pair, and reducing according to the compatible modulus;

to thereby yield a message encrypted with the first key of the second key pair,

wherein the modulus (n) for a respective key pair is a composite number, constructed by multiplying two large numbers, derived from prime numbers, (p) and (q) together, and the respective first and second keys (d) and (e) of a respective key pair are related to each other and the modulus (n) in the following way:

$$d=e^{-1} \bmod((p-1)(q-1)).$$

14. The method according to claim **1**,

wherein said defining step comprises providing information encrypted with an RSA-type asymmetric key encryption algorithm encrypted with a first RSA-type key; and

said processing step comprises processing the provided information with a modified RSA-type asymmetric key algorithm using a composite key comprising a function of a complementary key to said first RSA-type key and a second RSA-type key.

15. The method according to claim **1**, further comprising the steps of:

receiving, by an intermediary, an identifier of desired information and accounting information for a receiver and accounting for a transaction involving the information;

transmitting an identifier of desired information and an intended recipient from the intermediary to a sender;

negotiating, by the intermediary, the new cryptographic comprehension function for the information sent by the sender to the receiver, without providing the intermediary with information to decrypt either the information in accordance with the cryptographic comprehension function or the processed information in accordance with the new cryptographic comprehension function; and

transmitting the processed information from the sender to the receiver.

16. A method for communicating information between a first party and a second party, comprising the steps of:

receiving, by an intermediary, an identifier of desired information, an authentication of the first party, and accounting information for a transaction involving the information, from the first party;

generating, by the intermediary, a transcoding key for converting an encrypted file at the second party to a new encryption formation, having as components a decryption key for the encrypted file and a new encryption key;

receiving, by the first party, the encrypted file having the new encryption format; and

decrypting the encrypted file having the new encryption format with a decryption key associated with the transcoding key,

wherein at least one of:

an ability to decrypt the encrypted file having the new encryption format with the decryption key is sensitive to a dynamic parameter; and

the encrypted content does not pass through the intermediary, and the intermediary does not possess sufficient information for decrypting the encrypted file having the new encryption format.

17. The method according to claim **16**, wherein an intermediary provides information defining the transcoding key for said decrypting step, but does not have sufficient information to decrypt the encrypted file.

18. The method according to claim **16**, wherein an ability to decrypt the encrypted file having the new encryption format with the decryption key is sensitive to a dynamic parameter.

19. The method according to claim **16**, wherein the intermediary does not possess sufficient information for decrypting the encrypted file having the new encryption format.

20. A method for processing information, comprising the steps of:

storing a record in a first encrypted format;

receiving a transaction request for the record from a requestor;

financially accounting for a transaction involving the record;

securely negotiating between the requestor and an intermediary, a decryption key for the record, said decryption key being different than an associated decryption key for said record in said first encrypted format;

converting the record to a second encrypted format, without being represented in an unencrypted state during transition from the first encrypted format to the second encrypted format, and without providing sufficient information at the site of conversion to enable decryption of the record from the first or second encrypted format before, during or after conversion, such that the negotiated decryption key is selectively operative to decrypt the record in the second encrypted format;

communicating the record encrypted in the second encrypted format to the requestor, without passing the record through the intermediary; and

decrypting the record in the second encrypted format by the requester based on the negotiated decryption key.

21. The method according to claim **20**, wherein the intermediary is not provided with sufficient information to decrypt the record in the second encrypted format.

22. A method for processing information, comprising the steps of:

defining a cryptographic comprehension function adapted for making at least a portion of an information record incomprehensible, said cryptographic comprehension function having associated asymmetric cryptographic keys;

generating, by an intermediary, a transcoding key for converting information encrypted with said cryptographic comprehension function to information encrypted with a new cryptographic comprehension function, having as components a decryption key for the encrypted information and a new encryption key;

processing the information encrypted with said cryptographic comprehension function with the transcoding key to invert the cryptographic comprehension function and impose the new cryptographic comprehension function, without revealing the portion of the information record in an intermediate step;

providing a first communications channel between a first and second party;

providing a second communications channel between each of the first and second parties and the intermediary;

communicating, by the intermediary through the second communications channel, with at least one of the first and second parties, information necessary for comprehension of the incomprehensible portion of the information record communicated over the first communications channel, wherein at least one of either: (a) the intermediary is neither provided with the portion of the information in a comprehensible or incomprehensible form, nor sufficient decryption information for the comprehension of the incomprehensible portion of the information record or (b) the ability of the information necessary for comprehension of the incomprehensible portion of the record changes dynamically; and

communicating the processed information over the first communications channel between the first and second parties.

23. The method according to claim **22**, wherein said new cryptographic comprehension function has a cryptographic security based on an asymmetry between a difficulty of

exponentiation of a message with a number derived from at least two large prime numbers, and a factoring thereof.

24. The method according to claim **22**, wherein the ability of the information necessary for comprehension of the incomprehensible portion of the record changes dynamically.

25. The method according to claim **22**, wherein the ability of the information necessary for comprehension of the incomprehensible portion of the record changes as a function of time.

* * * * *