US006175921B1

(12) **United States Patent**
Rosen

(10) **Patent No.: US 6,175,921 B1**
(45) **Date of Patent: *Jan. 16, 2001**

(54) **TAMPER-PROOF DEVICES FOR UNIQUE IDENTIFICATION**

(75) Inventor: **Sholom S. Rosen**, New York, NY (US)

(73) Assignee: **Citibank, N.A.**, New York, NY (US)

(*) Notice: This patent issued on a continued prosecution application filed under 37 CFR 1.53(d), and is subject to the twenty year patent term provisions of 35 U.S.C. 154(a)(2).

Under 35 U.S.C. 154(b), the term of this patent shall be extended for 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **08/895,395**

(22) Filed: **Jul. 16, 1997**

Related U.S. Application Data

(62) Division of application No. 08/730,158, filed on Oct. 23, 1996, now Pat. No. 5,703,949, which is a continuation of application No. 08/575,699, filed on Dec. 19, 1995, now abandoned, which is a division of application No. 08/234,461, filed on Apr. 28, 1994, now Pat. No. 5,557,518.

(51) **Int. Cl.**^{7} **H04L 9/30**

(52) **U.S. Cl.** **713/173**; 713/156; 713/159; 713/168; 380/279; 380/283; 705/67

(58) **Field of Search** 380/4, 23, 279, 380/283; 713/156, 159, 168, 173; 705/67; 235/379, 380; 340/825.3, 825.34

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,443,027	4/1984	McNeely et al. .	
4,453,074	6/1984	Weinstein .	
4,454,414	6/1984	Benton .	
4,529,870	7/1985	Chaum .	
4,634,807	1/1987	Chorley et al. .	
4,644,493	2/1987	Chandra et al. .	
4,663,664	5/1987	Ragan et al. .	
4,682,223	7/1987	Ragan et al. .	
4,682,224	7/1987	Ragan et al. .	
4,723,284	2/1988	Munck et al. .	
4,794,644	12/1988	Philip et al. .	
4,799,156	1/1989	Shavit et al. .	
4,817,140	3/1989	Chandra et al. .	
4,864,615	9/1989	Bennett et al. .	
4,868,877	9/1989	Fischer .	
4,876,716	10/1989	Okamoto .	
4,879,747	11/1989	Leighton et al. .	
4,888,800	12/1989	Marshall et al. .	
4,910,774 *	3/1990	Barakat	380/23
4,916,738	4/1990	Chandra et al. .	
4,926,480	5/1990	Chaum .	
4,933,971	6/1990	Bestock et al. .	
4,941,173	7/1990	Boule et al. .	
4,956,863	9/1990	Goss .	
4,972,175	11/1990	MacPherson .	
4,977,595	12/1990	Ohta et al. .	
4,993,069	2/1991	Matyas et al. .	
4,999,806	3/1991	Chernow et al. .	
5,001,752	3/1991	Fischer .	

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

0 172 670 A2	2/1986	(EP) .
0 380 377 B1	8/1990	(EP) .
4 191 06 A1	3/1991	(EP) .
0 474 360 A2	3/1992	(EP) .
0 569 816 A2	11/1993	(EP) .
22 57 55 7	1/1993	(GB) .
4-64129	2/1992	(JP) .
9308545	4/1993	(WO) .
9401825	1/1994	(WO) .

OTHER PUBLICATIONS

"Online Cash Checks", Chuam, D.; *Advances in Cryptology* Eurocrypt '89 Qiusquarter & J. Vandewalle (Eds.) Springer–Verlag, pp. 288–293.

"Achieving Electronic Privacy", Chaum D.; *Scientific American,* Aug. 1992, pp. 96–101.

"Value Exchange Systems Enabling Security and Unobservability", Burk, H., et al., *Computer & Security,* 9 (1990), pp. 715–721.

"Proxy–Based Authorization and Accounting for Distributed Systems", Neuman, D. Clifford; *Proceedings of the 13th International Conference on Distributed Computing Systems,* Pittsburgh, May 1993.

"Le paiement électronique", P. Rémery, J.C. Pailles and F. Lay, *L'Echo des Recherches,* No. 134 4 trimester 1988 (with English–language translation).

"Padlock", D. Everett, *Computer Bulletin,* Mar. 1985, pp. 16–17.

"ABYSS: A Trusted Architecture for Software Protection", S.R. White and L. Comerford, *IEEE,* 1987.

(List continued on next page.)

Primary Examiner—Pinchus M. Laufer
Assistant Examiner—Hrayr D. Sayadian
(74) *Attorney, Agent, or Firm*—Morgan & Finnegan, LLP

(57) **ABSTRACT**

A system for open electronic commerce having a customer trusted agent securely communicating with a first money module, and a merchant trusted agent securely communicating with a second money module. Both trusted agents are capable of establishing a first cryptographically secure session, and both money modules are capable of establishing a second cryptographically secure session. The merchant trusted agent transfers electronic merchandise to the customer trusted agent, and the first money module transfers electronic money to the second money module. The money modules inform their trusted agents of the successful completion of payment, and the customer may use the purchased electronic merchandise. A certificate data signed by a trusted authority is stored in a tamper proof electronic processing device, which certificate includes a unique device ID and a public key of the device, in addition to device owner ID data. The processing device is programed to validate credential data received from other such processing devices.

8 Claims, 91 Drawing Sheets

U.S. PATENT DOCUMENTS

5,005,200		4/1991	Fischer .	
5,081,678		1/1992	Kaufman et al. .	
5,109,413		4/1992	Comerford et al. .	
5,117,457		5/1992	Comerford et al. .	
5,131,039		7/1992	Chaum .	
5,144,663		9/1992	Kudelski et al. .	
5,148,534		9/1992	Comerford .	
5,162,989		11/1992	Matsuda .	
5,177,791		1/1993	Yeh et al. .	
5,185,717		2/1993	Mori .	
5,200,999	*	4/1993	Matyas et al.	380/25
5,202,921		4/1993	Herzberg et al. .	
5,221,838		6/1993	Gutman et al. .	
5,247,576		9/1993	Bright .	
5,247,578		9/1993	Pailles et al. .	
5,265,164	*	11/1993	Matyas et al.	380/30
5,276,311		1/1994	Hennige .	
5,276,736		1/1994	Chaum .	
5,282,248		1/1994	Dejoy .	
5,301,247		4/1994	Rasmussen et al. .	
5,305,200		4/1994	Hartheimer et al. .	
5,319,705		6/1994	Halter et al. .	
5,389,738	*	2/1995	Piosenka et al.	174/52.4
5,396,558	*	3/1995	Ishiguro et al.	380/25
5,416,840		5/1995	Cane et al. .	
5,440,634		8/1995	Jones et al. .	
5,448,638		9/1995	Johnson et al. .	
5,453,601		9/1995	Rosen .	
5,473,692		12/1995	Davis .	
5,481,715		1/1996	Hamilton et al. .	
5,490,251		2/1996	Clark et al. .	
5,511,121		4/1996	Yacobi .	
5,519,778		5/1996	Leighton .	
5,539,828		7/1996	Davis .	
5,557,518	*	9/1996	Rosen	364/408
5,568,552		10/1996	Davis .	
5,621,797		4/1997	Rosen .	
5,642,419		6/1997	Rosen .	
5,703,949		12/1997	Rosen .	
5,878,139		3/1999	Rosen .	

OTHER PUBLICATIONS

"Public Protection of Software", A. Herzberg and S.S. Pinter, *ACM Transactions on Computer Systems,* vol. 5, No. 4, Nov. 1987, pp. 371–393.

"Security Without Identification: Card Computers To Make Big Brother Obsolete", D. Chaum, 1987.

"Internet Billing Service Design and Prototype Implementation", Marvin A Sirbu, *IMA Intellectual Property Project Proceedings,* vol. 1, Issue, Jan. 1994.

"Dyad: A System for Using Physically Secure Coprocessors", J.D. Tygar and B. Yee, School of Computer Science, Carnegie Mellon Univ., Pittsburgh, PA.

"Trusted Devices as applied to Corporate Key Escrow", F. Sudia, Jan. 14, 1994, Bankers Trust Co.

"Wavemeter Chip Provides Digital Money", M. Slater, *Microprocessor Report,* vol. 8, No. 5, Apr. 18, 1994.

"Data Networks and Open System Communications Directory/Information Technology—Open Systems Interconnection—The Directory: Authentication Framework," ITU–Recommendation X.509, Nov. 1993.

"Anonymous Internet Mercantile Protocol", AT&T Bell Laboratories, Draft: Mar. 17, 1994, pp. 1–16, David M. Kristol, Steven H. Low, Nicholas F. Maxemchunk.

Literature of Microcomputer [II], edited by Nihon Denshi Kogyo Sinko Kyokai (Mar., 1988), pp. 190–217 (Japanese Language).

"Universal Electronic Cash", Tatsuaki Okamoto and Kazuo Ohta, CRYPTO '91, (Sessions 8: Applications and Implementations; pp. 8–7 through 8–13).

"Limitations of the Kerberos Authentication System", Steven M. Bellovin and Michael Merritt, USENIX—Winter '91 (1–15).

"Applied Cryptography: Protocols, Algorithms, and Source Code in C", Bruce Schneier, John Wiley & Sons, Inc. (417–429) ISBN 0–471–59756–2; QA76.9.A25S35 1993.

"An Architecture for Practical Delegation in a Distributed System", Morrie Gasser, Ellen McDermott, IEEE Computer Society Press, IEEE Computer Society Symposium on Research in Security and Privacy, May 7–9, 1990.

"Practical Uses of Synchronized Clocks in Distributed Systems", Barbara Liskov, ACM Press, 10th Annual ACM Symposium on Principles of Distributed Computing, Aug. 19–21, 1991, ISBN 0–89791–439–2.

"SPX: Global Authentication Using Public Key Certificates", Joseph J. Tardo and Kannan Alagappan, IEEE 1991 (CH2986–8/91/0000/0232).

"The Digital Distributed System Security Architecture", Morrie Gasser, et al., Nat'l. Inst. of Standards and Tech./ Nat'l Computer Security Ctr., 12th National Computer Security Conferences, Baltimore, MD Oct. 10–13, 1989.

U.S. application No. 09/138,107 Rosen filed Aug. 21, 1998.

* cited by examiner

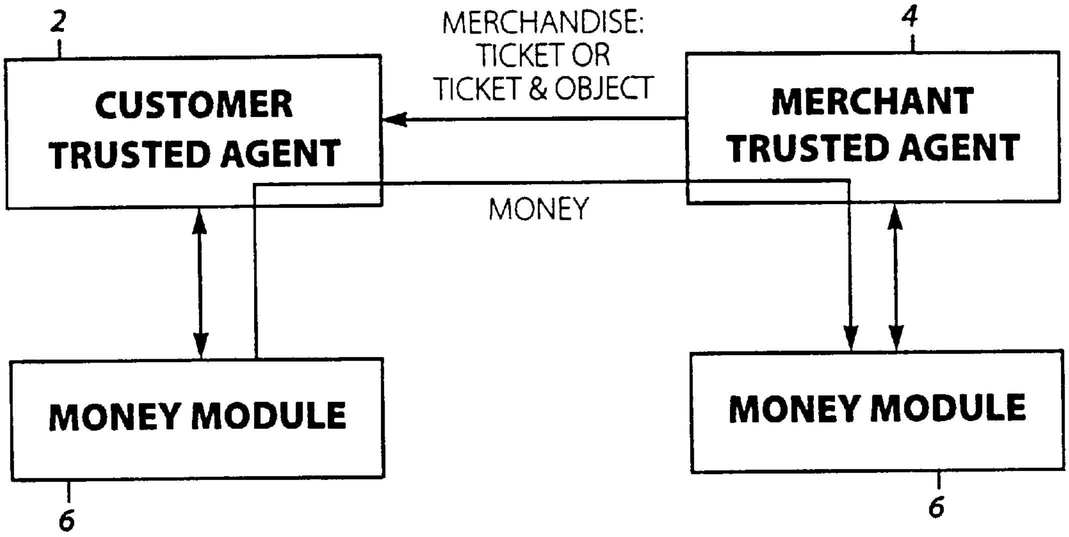
2
CUSTOMER TRUSTED AGENT
MERCHANDISE: TICKET OR TICKET & OBJECT
4
MERCHANT TRUSTED AGENT
MONEY
MONEY MODULE
MONEY MODULE
6
6

Figure 1

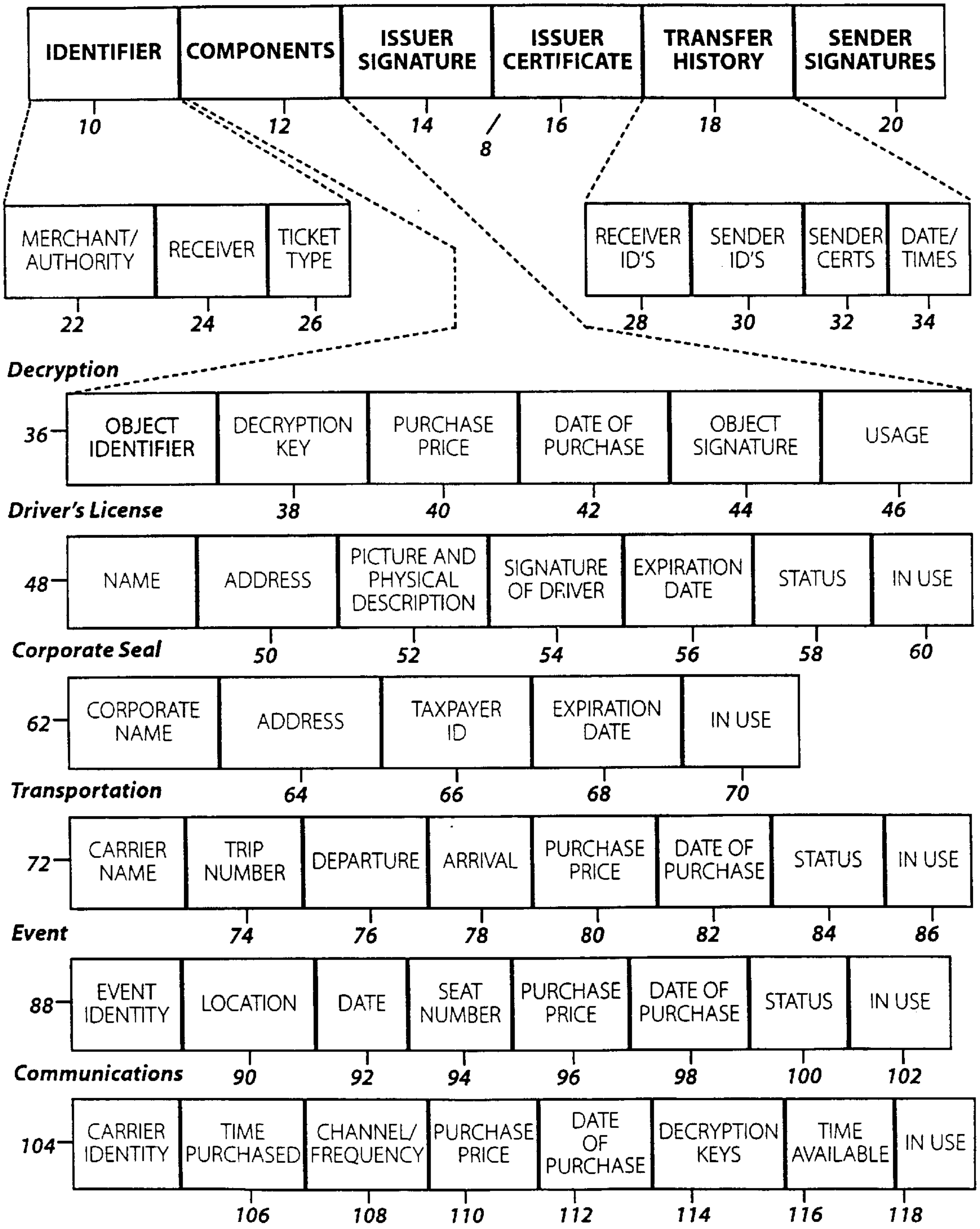
IDENTIFIER
COMPONENTS
ISSUER SIGNATURE
ISSUER CERTIFICATE
TRANSFER HISTORY
SENDER SIGNATURES
10
12
14
8
16
18
20
MERCHANT/ AUTHORITY
RECEIVER
TICKET TYPE
22
24
26
RECEIVER ID'S
SENDER ID'S
SENDER CERTS
DATE/ TIMES
28
30
32
34
Decryption
36
OBJECT IDENTIFIER
DECRYPTION KEY
PURCHASE PRICE
DATE OF PURCHASE
OBJECT SIGNATURE
USAGE
Driver's License
38
40
42
44
46
48
NAME
ADDRESS
PICTURE AND PHYSICAL DESCRIPTION
SIGNATURE OF DRIVER
EXPIRATION DATE
STATUS
IN USE
Corporate Seal
50
52
54
56
58
60
62
CORPORATE NAME
ADDRESS
TAXPAYER ID
EXPIRATION DATE
IN USE
Transportation
64
66
68
70
72
CARRIER NAME
TRIP NUMBER
DEPARTURE
ARRIVAL
PURCHASE PRICE
DATE OF PURCHASE
STATUS
IN USE
Event
74
76
78
80
82
84
86
88
EVENT IDENTITY
LOCATION
DATE
SEAT NUMBER
PURCHASE PRICE
DATE OF PURCHASE
STATUS
IN USE
Communications
90
92
94
96
98
100
102
104
CARRIER IDENTITY
TIME PURCHASED
CHANNEL/ FREQUENCY
PURCHASE PRICE
DATE OF PURCHASE
DECRYPTION KEYS
TIME AVAILABLE
IN USE
106
108
110
112
114
116
118

Figure 2

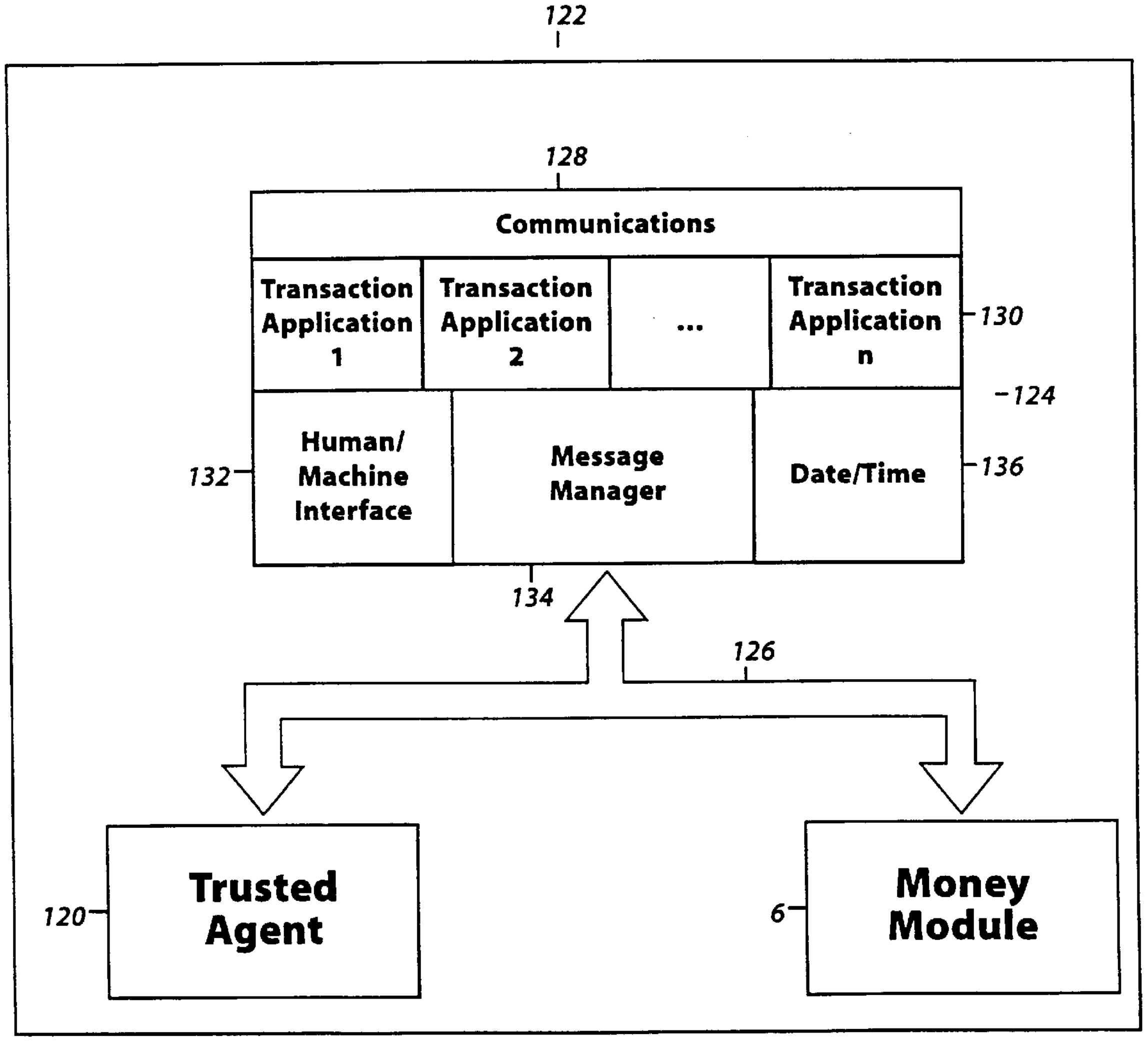
122
128
Communications
Transaction Application 1
Transaction Application 2
...
Transaction Application n
130
124
132
Human/ Machine Interface
Message Manager
Date/Time
136
134
126
Trusted Agent
120
6
Money Module

Figure 3

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE