US006985583B1

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

(10) **Patent No.: US 6,985,583 B1**
(45) **Date of Patent: Jan. 10, 2006**

(54) **SYSTEM AND METHOD FOR AUTHENTICATION SEED DISTRIBUTION**

(75) Inventors: **John G. Brainard**, Sudbury, MA (US); **Burton S. Kaliski, Jr.**, Wellesley, MA (US); **Magnus Nyström**, Concord, MA (US); **Ronald L. Rivest**, Arlington, MA (US)

(73) Assignee: **RSA Security Inc.**, Bedford, MA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/304,775**

(22) Filed: **May 4, 1999**

(51) **Int. Cl.**
H04L 9/00 (2006.01)
H04L 9/32 (2006.01)

(52) **U.S. Cl.** **380/44**; 380/277; 713/168; 713/169; 713/171; 713/176; 713/200

(58) **Field of Classification Search** 713/168–176; 380/44, 277
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,104,694	A	8/1978	Hargrove	
4,145,568	A	3/1979	Ehrat	
4,145,569	A	3/1979	Ehrat	
4,238,854	A *	12/1980	Ehrsam et al.	713/165
4,317,957	A	3/1982	Sendrow	
4,320,387	A	3/1982	Powell	
4,369,332	A	1/1983	Campbell, Jr.	
4,438,824	A	3/1984	Mueller-Schloer	
4,471,216	A	9/1984	Herve	
4,509,093	A	4/1985	Stellberger	
4,536,647	A	8/1985	Atalla et al.	
4,543,657	A	9/1985	Wilkinson	
4,575,621	A	3/1986	Dreifus	
4,578,530	A	3/1986	Zeidler	
4,582,434	A	4/1986	Plangger et al.	
4,599,489	A	7/1986	Cargile	
4,605,820	A	8/1986	Campbell, Jr.	
4,609,777	A	9/1986	Cargile	
4,614,861	A	9/1986	Pavlov et al.	

(Continued)

FOREIGN PATENT DOCUMENTS

EP 0140013 B1 5/1985

(Continued)

OTHER PUBLICATIONS

FIPS Publ. 190, "Guideline for the use of advanced authentication technology alternatives", Sep. 28, 1994, section 4; section 4.4.2.1 particularly.*

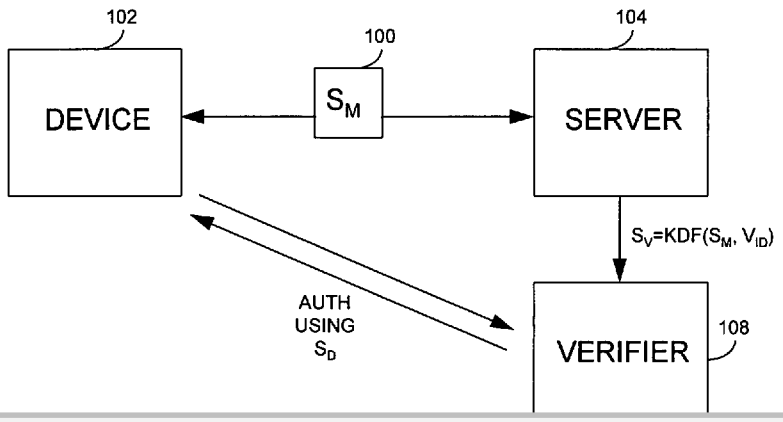
(Continued)

Primary Examiner—Ayaz Sheikh
Assistant Examiner—Ronald Baum
(74) *Attorney, Agent, or Firm*—Wilmer Cutler Pickering Hale and Dorr LLP

(57) **ABSTRACT**

In one embodiment of a user authentication system and method according to the invention, a device shares a secret, referred to as a master seed, with a server. The device and the server both derive one or more secrets, referred to as verifier seeds, from the master seed, using a key derivation function. The server shares a verifier seed with one or more verifiers. The device, or an entity using the device, can authenticate with one of the verifiers using the appropriate verifier seed. In this way, the device and the verifier can share a secret, the verifier seed for that verifier, without that verifier knowing the master seed, or any other verifier seeds. Thus, the device need only store the one master seed, have access to the information necessary to correctly derive the appropriate seed, and have seed derivation capability. A verifier cannot compromise the master seed, because the verifier does not have access to the master seed.

35 Claims, 5 Drawing Sheets



U.S. PATENT DOCUMENTS

4,720,860	A		1/1988	Weiss
4,731,841	A		3/1988	Rosen et al.
4,800,590	A		1/1989	Vaughan
4,819,267	A		4/1989	Cargile et al.
4,849,613	A		7/1989	Eisele
4,856,062	A		8/1989	Weiss
4,885,778	A		12/1989	Weiss
4,890,323	A		12/1989	Beker et al.
4,928,098	A		5/1990	Dannhaeuser
4,933,971	A	*	6/1990	Bestock et al. 380/44
4,944,008	A		7/1990	Piosenka et al.
4,998,279	A		3/1991	Weiss
5,016,276	A		5/1991	Matumoto et al. 380/45
5,023,908	A		6/1991	Weiss
5,046,125	A		9/1991	Takizawa
5,058,161	A		10/1991	Weiss
5,097,505	A		3/1992	Weiss
5,101,430	A		3/1992	Periou
5,168,520	A		12/1992	Weiss
5,180,902	A		1/1993	Schick et al.
5,206,905	A		4/1993	Lee et al.
5,237,614	A		8/1993	Weiss
5,280,527	A		1/1994	Gullman et al.
5,347,580	A	*	9/1994	Molva et al. 713/159
5,361,062	A		11/1994	Weiss et al.
5,367,572	A		11/1994	Weiss
5,479,512	A		12/1995	Weiss
5,485,519	A		1/1996	Weiss
5,513,263	A	*	4/1996	White et al. 380/44
5,539,824	A	*	7/1996	Bjorklund et al. 380/249
5,592,553	A		1/1997	Guski et al.
5,655,077	A	*	8/1997	Jones et al. 713/201
5,657,388	A		8/1997	Weiss
5,717,756	A		2/1998	Coleman
5,732,133	A		3/1998	Mark
5,737,421	A		4/1998	Audebert
5,748,734	A	*	5/1998	Mizikovsky 380/247
5,802,176	A		9/1998	Audebert
5,841,864	A	*	11/1998	Klayman et al. 713/171
5,887,065	A		3/1999	Audebert
5,937,068	A		8/1999	Audebert
6,078,888	A	*	6/2000	Johnson, Jr. 705/1
6,141,760	A		10/2000	Abadi et al.
6,295,359	B1	*	9/2001	Cordery et al. 380/44
6,338,140	B1	*	1/2002	Owens et al. 713/168

FOREIGN PATENT DOCUMENTS

EP	0148960	B1	7/1985
EP	0566811	A1	10/1993
EP	0678836	B1	10/1995
FR	2607544		6/1988
JP	59-119630		5/1991
JP	2835433		6/1997
JP	2884338		4/1999
WO	88/06826		9/1988

OTHER PUBLICATIONS

Chevassut, O., et al, "One-time Verifier based Encrypted Key Exchange", Lawrence Berkeley National Lab., Springer-Verlag 2004-2005, entire document.*

Kim, Y., et al, "Secure authentication system that generates seed from biometric information", Feb. 10, 2005, Optical Society of America, Applied Optics, vol. 44, No. 5, entire article.*

American National Standard for Financial Services. "Financial Services Key Management Using the DEA," American Bankers Association, copyright 1992, 1999, pp. i-iii, 1-9, 34-52.

RSA Laboratories, a division of RSA Data Security, Inc. "PKCS #5 v2.0: Password-Based Cryptography Standard." Mar. 25, 1999, copyright 1991-1999, pp. 1-30.

Standard Specifications for Public Key Cryptography, IEEE P 1363 / D 13 (Draft Version 13), Institute of Electrical and Electronics Engineers, Inc., New York, NY, Nov. 12, 1999, pp. 1, 4-6, 53-57, 71-73.

Freier, et al. The SSL Protocol, Version 3.0, http://home.netscape.com/eng/ssl3/3-SPEC.htm, Mar. 1996, pp. 1-26, and Table of Contents, http://home.netscape.com/eng/ssl3/ssl-toc.html, pp. 1-3.

European Patent Office, European Search Report, International Application EP 00 30 3741, date of completion of search Jan. 16, 2002, 2 pages.

Ferreira, "The Smart Card: A High Security Tool in EDP", Philips Telecommunications and Data Systems Review, Philips Telecommunicatie Industrie N.V. Hilversum, NL, Sep. 1989, vol. 47, No. 3, pp. 1-19.

Shamir,"Identity-Based Cryptosystems and Signature Schemes", Lecture Notes in Computer Science, Springer Verlag, New York, NY, US, 1985, pp. 47-53.

* cited by examiner

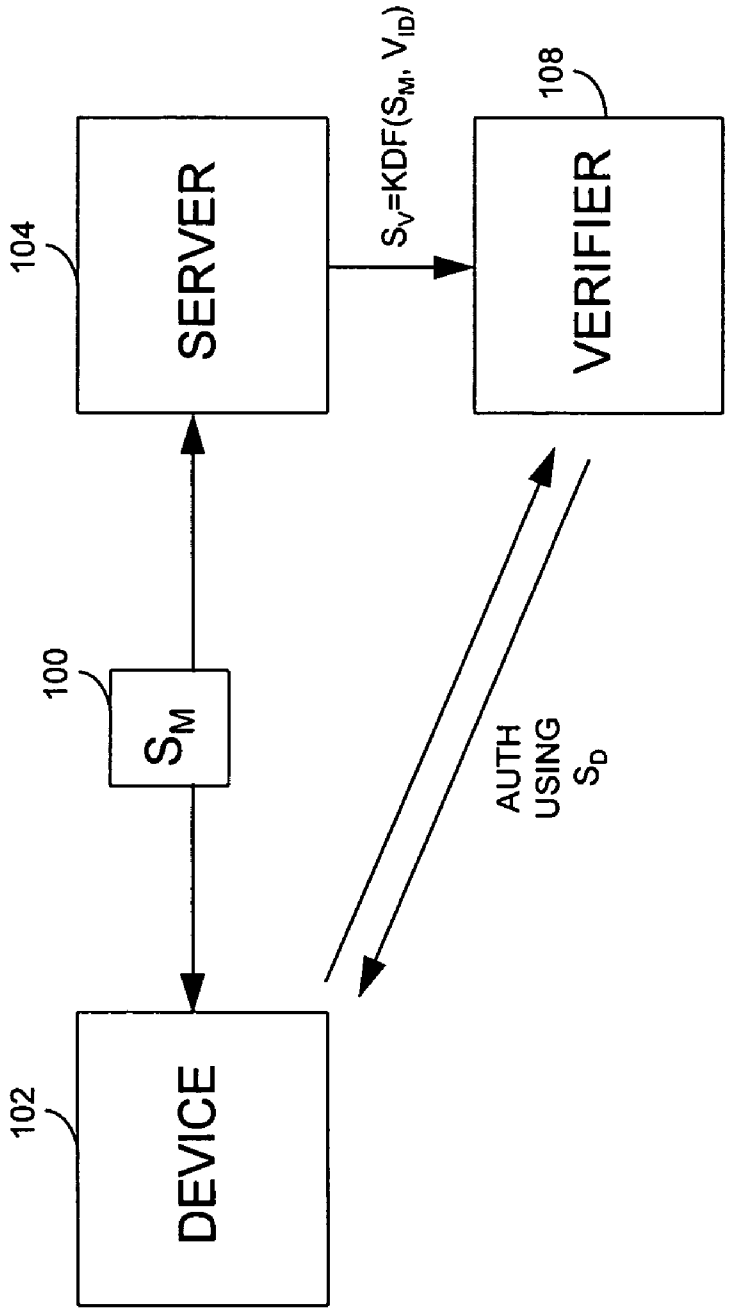


FIG. 1

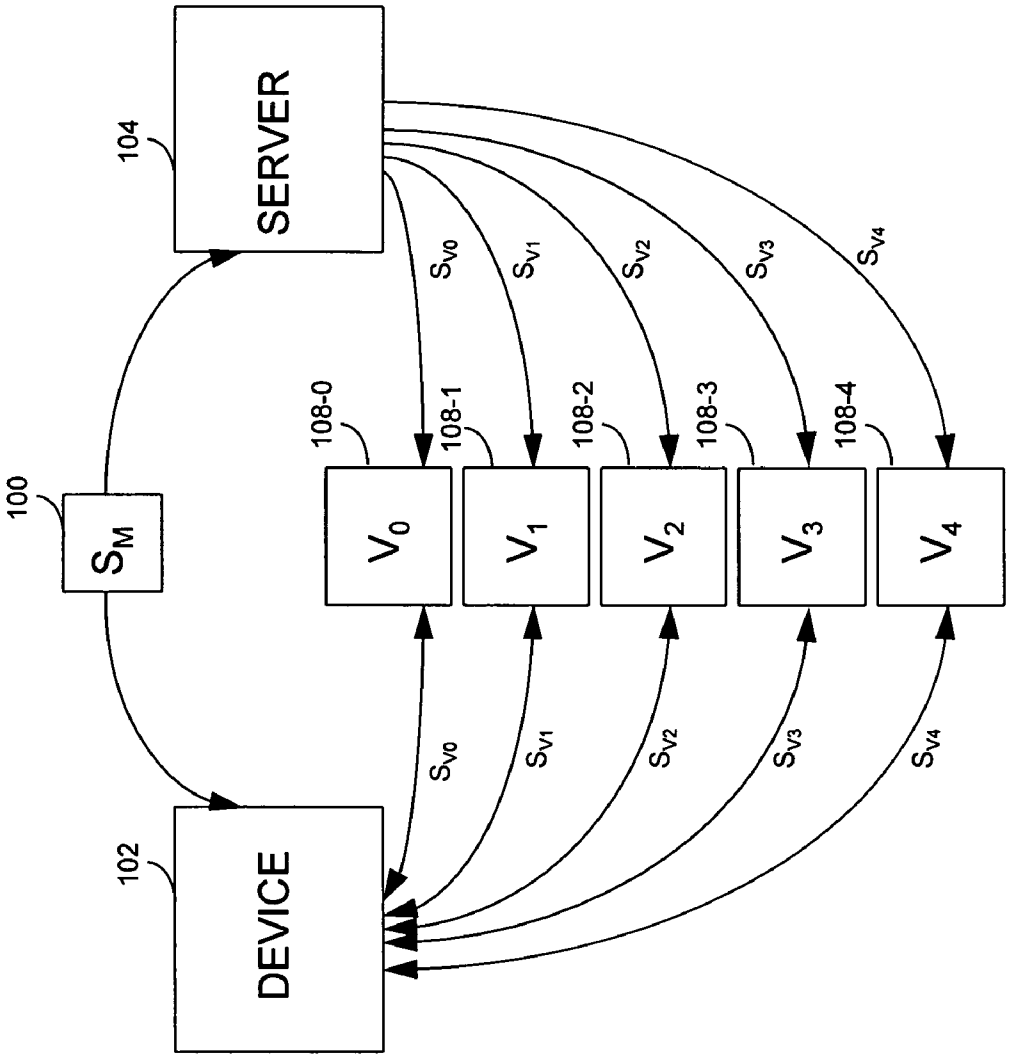


FIG. 2

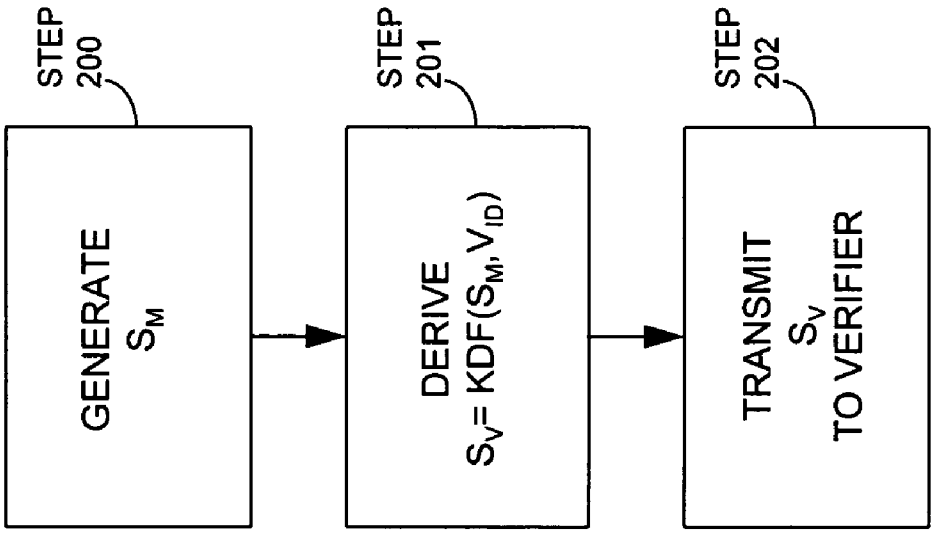


FIG. 3

DOCKET ALARM

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.