US005799086A

United States Patent [19]

Sudia

[11] **Patent Number: 5,799,086**

[45] **Date of Patent: Aug. 25, 1998**

[54] **ENHANCED CRYPTOGRAPHIC SYSTEM AND METHOD WITH KEY ESCROW FEATURE**

[75] Inventor: **Frank Wells Sudia**, New York, N.Y.

[73] Assignee: **CertCo LLC**, New York, N.Y.

[21] Appl. No.: **803,176**

[22] Filed: **Feb. 19, 1997**

Related U.S. Application Data

[60] Division of Ser. No. 272,203, Jul. 8, 1994, abandoned, which is a continuation-in-part of Ser. No. 181,859, Jan. 13, 1994, abandoned.

[51] **Int. Cl.**^{6} **H04L 9/32**

[52] **U.S. Cl.** **380/23**; 380/30

[58] **Field of Search** 380/30, 23

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,200,770	4/1980	Hellman et al. .	
4,218,582	8/1980	Hellman et al. .	
4,405,829	9/1983	Rivest et al. .	
4,868,877	9/1989	Fischer .	
4,995,082	2/1991	Schnorr .	
5,001,752	3/1991	Fischer .	
5,005,200	4/1991	Fischer .	
5,136,643	8/1992	Fischer .	
5,150,411	9/1992	Maurer .	
5,164,988	11/1992	Matyas et al. .	
5,199,070	3/1993	Matsuzaki et al. .	
5,214,700	5/1993	Pinkas et al. .	
5,214,702	5/1993	Fischer .	
5,222,140	6/1993	Beller et al. .	
5,261,002	11/1993	Perlman et al. .	
5,276,737	1/1994	Micali .	
5,313,521	5/1994	Torii et al. .	
5,315,658	5/1994	Micali .	
5,371,794	12/1994	Diffie et al.	380/21
5,396,558	3/1995	Ishiguro et al.	380/25
5,539,828	7/1996	Davis	380/50
5,557,518	9/1996	Rosen	364/408

OTHER PUBLICATIONS

American National Standard X9.30, "Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry: Part 1: The Digital Signature Algorithm (DSA)" (American Bankers Assn., Washington, D.C., 1993).

American National Standard X9.30, "Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry: Part 2: The Secure Hash Algorithm (SHA)" (American Bankers Assn., Washington, D.C., 1993).

American National Standard X9.30, "Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry: Part 3: Certificate Management for DSA" (American Bankers Assn., Washington, D.C., 1993).

Silvio Micali, "Fair Public Key Cryptosystems", Laboratory for Computer Science of the Massachusetts Institute of Technology,. Oct. 13, 1993.

Donn B. Parker, "Crypto and Avoidance of Business Information Anarchy" First Annual AC Conference on Computer and Communication Security, Nov. 3–5, Reston, VA.

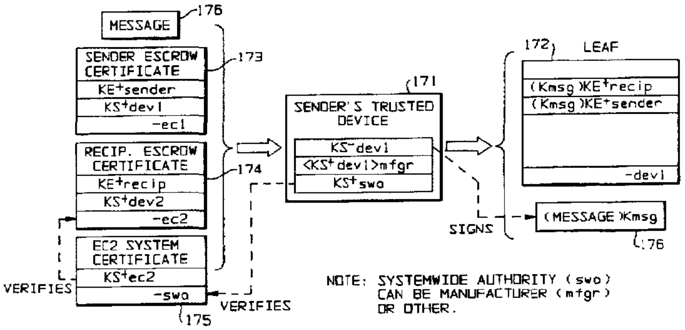
(List continued on next page.)

Primary Examiner—Gilberto Barron, Jr.
Attorney, Agent, or Firm—Steptoe & Johnson LLP

[57] **ABSTRACT**

A cryptographic system with key escrow feature that uses a method for verifiably splitting user's private encryption keys into components and for sending those components to trusted agents chosen by the particular users is provided. The system uses public key certificate management, enforced by a chip device that also self-certifies. The methods for key escrow and receiving an escrow certificate are applied to register a trusted device with a trusted third party and to receive authorization from that party enabling the device to communicate with other trusted devices. The methods for key escrow also provide assurance that a trusted device will engage in electronic transactions in accordance with predetermined rules.

12 Claims, 25 Drawing Sheets



NOTE: SYSTEMWIDE AUTHORITY (swo) CAN BE MANUFACTURER (mfgr) OR OTHER.

SEND ENCRYPTED MESSAGE WITH MCH (OVERVIEW)

OTHER PUBLICATIONS

CCITT Recommendation X.509, "The Directory—Authentication Framework", International Standards Organization (ISO), Melbourne, Australia 1988.

Dorothy E. Denning, "The Clipper Encryption System", American Scientist, Jul.–Aug., 1993, pp. 319–323.

Martin E. Hellman, "Commercial Encryption", IEEE Network Magazine, Apr. 1987, vol. 1, No. 2, pp. 6–10.

David B. Newman, Jr., Jim K. Omura and Raymond L. Pickholtz, "Public Key Management for Network Security", IEEE Network Magazine, Apr. 1987, vol. 1, No. 2, pp. 11–16.

DIFFIE-HELLMAN AND MICALI ABBREVIATIONS

x	RECIPIENTS PRIVATE KEY (EXPONENT)
x1...n	NUMBERED FRAGMENTS OF PRIVATE KEY
xi	i-th FRAGMENT OF PRIVATE KEY
y	SENDER'S EPHEMERAL PRIVATE KEY (EXPONENT)
a	PUBLIC BASE NUMBER
P	PUBLIC PRIME MODULUS NUMBER
DHx	INTERMEDIATE NUMBER, $= a^{x} \bmod P$
DHy	INTERMEDIATE NUMBER, $= a^{y} \bmod P$
Kdh	DIFFIE-HELLMAN DERIVED MESSAGE KEY
V1...n	MICALI INTERMEDIATE NUMBER, $= a^{xi} \bmod P$

OTHER SYMMETRIC KEY ABBREVIATIONS

k_{msg}	RANDOM OR DERIVED MESSAGE KEY
M	PLAINTEXT MESSAGE
C	CIPHERTEXT MESSAGE

FIG. 1A

FIG. 1B GENERAL ASSYMETRIC KEY NOTATION

	PUBLIC	PRIVATE
SIGNATURE	KS^{+}	KS^{-}
ENCRYPTION	KE^{+}	KE^{-}

FIG. 1C PUBLIC KEY CERTIFICATE NOTATION (EXAMPLE)

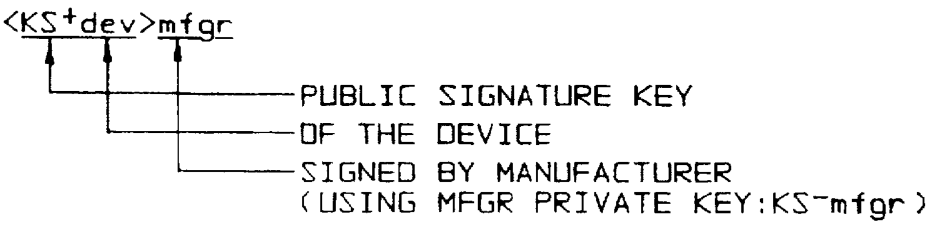

$\langle KS^{+}dev\rangle mfgr$
PUBLIC SIGNATURE KEY
OF THE DEVICE
SIGNED BY MANUFACTURER
(USING MFGR PRIVATE KEY: $KS^{-}mfgr$)

FIG. 1D

PUBLIC KEY ENCRYPTON
NOTATION (EXAMPLE)

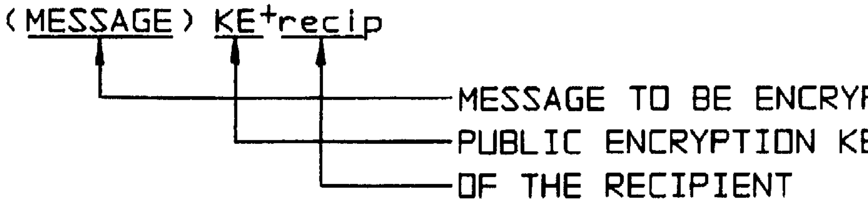


FIG. 1E SUFFIXES USED TO DENOTE KEY OWENERSHIP

box		LAW ENFORCEMENT DECODER BOX
ca	ca1...n	CERTIFYING AUTHORITY (FOR PUBLIC SIGNATURE K
dev		DTRUSTED DEVICE
ea	ea1...n	ESCROW AGENT
ec	ec1...n	ESCROW CENTER
mfgr	mfg1...n	MANUFACTURER OF THE TRUSTED DEVICE
owner		OWNER OF DEVICE (IF OTHER THAN USER)
recip		RECIPIENT OF A MESSAGE
sender		SENDER OF A MESSAGE
swa		SYSTEM-WIDE AUTHORITY
user	user1...n	USER OF THE TRUSTED DEVICE

FIG. 1F

SHORTHAND NOTATION - SIGNING

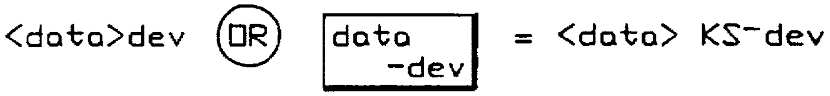


FIG. 1G

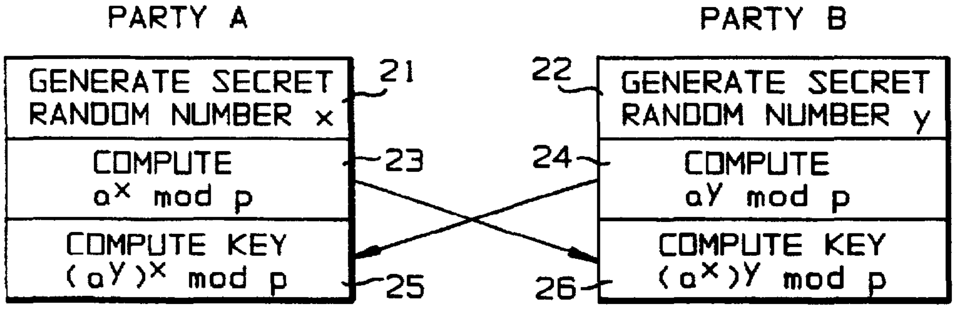
SHORTHAND NOTATION - ENCRYPTION

<data>sender = (data) KE^{+}sender

FIG. 2

INTERACTIVE DIFFIE-HELLMAN KEY DERIVATIVE

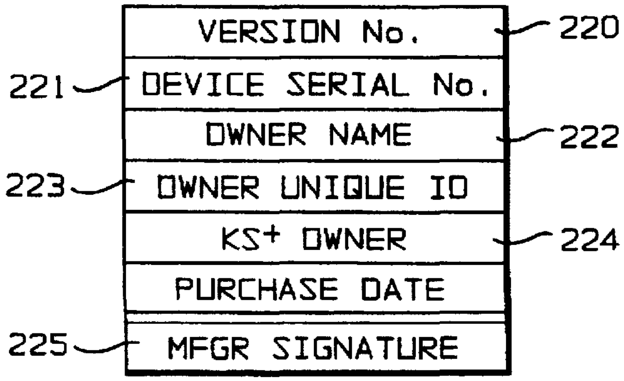
PRIOR AGREEMENT ON (NON-SECRET)
PRIME p AND VALUE a


PARTY A
PARTY B
GENERATE SECRET RANDOM NUMBER x
21
22
GENERATE SECRET RANDOM NUMBER y
COMPUTE a^x mod p
23
24
COMPUTE a^y mod p
COMPUTE KEY $(a^y)^x$ mod p
25
26
COMPUTE KEY $(a^x)^y$ mod p

COMMON KEY a^{xy} mod p KNOWN BY A AND B
BUT NOT DEDUCIBLE BY AN EAVESDROPPER

FIG. 22

DEVICE OWNER'S
CERTIFICATE (EXAMPLE)



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.

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

fastcase®
Smarter legal research.