CORRECTED VERSION*

SG 9700406-3

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) **International Patent Classification** 6 : H04L 9/32

A3

(11) **International Publication Number:** WO 96/02993

(43) **International Publication Date:** 1 February 1996 (01.02.96)

(21) **International Application Number:** PCT/US95/09076

(22) **International Filing Date:** 19 July 1995 (19.07.95)

(30) **Priority Data:**
08/277,438 19 July 1994 (19.07.94) US

(60) **Parent Application or Grant**
(63) Related by Continuation
US 08/277,438 (CIP)
Filed on 19 July 1994 (19.07.94)

(71) **Applicant** *(for all designated States except US)*: BANKERS TRUST COMPANY [US/US]; Four Albany Street, New York, NY 10006 (US).

(72) **Inventors; and**
(75) **Inventors/Applicants** *(for US only)*: SUDIA, Frank, W. [US/US]; Apartment 4B, 110 East 84th Street, New York, NY 10028 (US). SIRIPZKY, Brian [IE/US]; Apartment 2, 11410 Strand Drive, Rockville, MD 20852 (US).

(74) **Agents:** LAZAR, Dale, S. et al.; Cushman Darby & Cushman L.L.P., 1100 New York Avenue, N.W., Washington, DC 20005 (US).

(81) **Designated States:** AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TT, UA, UG, US, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, MW, SD, SZ, UG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) **Date of publication of the international search report:**
7 March 1996 (07.03.96)

RTMP copy

(54) **Title:** METHOD FOR SECURELY USING DIGITAL SIGNATURES IN A COMMERCIAL CRYPTOGRAPHIC SYSTEM

(57) **Abstract**

A system for securely using digital signatures in a commercial cryptographic system that allows industry-wide security policy and authorization information to be encoded into the signatures and certificates by employing attribute certificates to enforce policy and authorization requirements. Verification of policy and authorization requirements is enforced in the system by restricting acess to public keys to users who have digitally signed and agreed to follow rules of the system. These rules can also ensure that payment is made for public and private key usage. Additionally, users can impose their own rules and policy requirements on transactions in the system.

* (Referred to in PCT Gazette No. 14/1996, Section II)

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	GB	United Kingdom	MR	Mauritania
AU	Australia	GE	Georgia	MW	Malawi
BB	Barbados	GN	Guinea	NE	Niger
BE	Belgium	GR	Greece	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IE	Ireland	NZ	New Zealand
BJ	Benin	IT	Italy	PL	Poland
BR	Brazil	JP	Japan	PT	Portugal
BY	Belarus	KE	Kenya	RO	Romania
CA	Canada	KG	Kyrgystan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo			SE	Sweden
CH	Switzerland	KR	Republic of Korea	SI	Slovenia
CI	Côte d'Ivoire	KZ	Kazakhstan	SK	Slovakia
CM	Cameroon	LI	Liechtenstein	SN	Senegal
CN	China	LK	Sri Lanka	TD	Chad
CS	Czechoslovakia	LU	Luxembourg	TG	Togo
CZ	Czech Republic	LV	Latvia	TJ	Tajikistan
DE	Germany	MC	Monaco	TT	Trinidad and Tobago
DK	Denmark	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	US	United States of America
FI	Finland	ML	Mali	UZ	Uzbekistan
FR	France	MN	Mongolia	VN	Viet Nam
GA	Gabon				

9700406-3