PCT WORLD INTELLECTUAL PROPI International B

WO 9602993A3

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). SIRITZKY, 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)

(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.

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				

INTERNATIONAL SEARCH REPORT

Interr ial Application No
PCT/US 95/09076

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US,A,5 164 988 (MATYAS ET AL.) 17 November 1992 see column 4, line 42 - line 66 see column 11, line 1 - line 13 see column 13, line 58 - column 14, line 2 see column 21, line 49 - column 22, line 26	1,3-5, 13,15
A	EP,A,0 386 867 (FISCHER) 12 September 1990 see page 13, line 19 - page 14, line 35	1,3-5, 13,15
A	& US,A,5 005 200 (FISCHER) cited in the application	1,3-5, 13,15

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
10 January 1996	29. 01. 96

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Holper, G

INTERNATIONAL SEARCH REPORT

.nformation on patent family members

Inter ıal Application No
PCT/US 95/09076

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
US-A-5164988	17-11-92	CA-A-	2071413	01-05-93
		EP-A-	0539726	05-05-93
		JP-A-	5216411	27-08-93
EP-A-386867	12-09-90	US-A-	5005200	02-04-91
		AT-T-	113429	15-11-94
		AU-B-	620291	13-02-92
		AU-B-	4242589	13-09-90
		CA-A-	2000400	07-09-90
		DE-D-	69013541	01-12-94
		DE-T-	69013541	09-03-95
		EP-A-	0586022	09-03-94
		ES-T-	2036978	01-01-95
		JP-A-	2291043	30-11-90
		US-A-	5214702	25-05-93