(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 January 2000 (06.01.2000)

PCT

(10) International Publication Number
WO 00/01108 A3

(51) International Patent Classification[6]: G07F 7/10

(21) International Application Number: PCT/US99/13908

(22) International Filing Date: 21 June 1999 (21.06.1999)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/107,762 30 June 1998 (30.06.1998) US

(71) Applicant: **PRIVADA, INC.** [US/US]; Two North First Street, San Jose, CA 95113 (US).

(72) Inventor: **MCLAUGHLIN, Craig, Peter**; 7448 Brighton Court, Dublin, CA 94568 (US).

(74) Agents: **VAUGHAN, Daniel, E.** et al.; Park & Vaughan LLP, 702 Marshall Street, Suite 310, Redwood City, CA 94063 (US).

(81) Designated State *(national)*: CA.

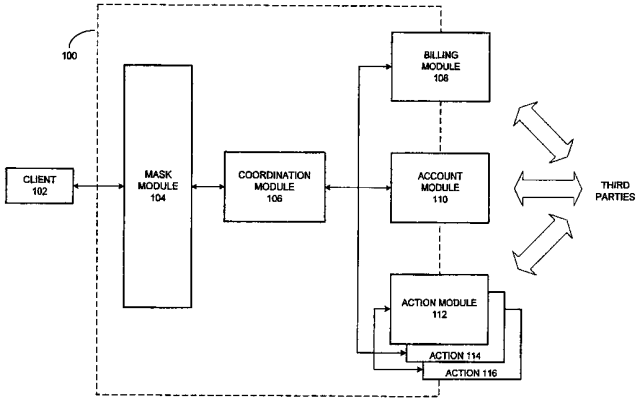
(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *with international search report*

(88) Date of publication of the international search report:
23 August 2001

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: BI-DIRECTIONAL, ANONYMOUS ELECTRONIC TRANSACTIONS



(57) Abstract: A system and methods are provided provided for processing bi-directional, anonymous or pseudo-anonymous user transactions, including electronic mail and electronic commerce. A first digital certificate is used to authenticate a user when he or she connects to the system to conduct a transaction. A second digital certificate is created to authenticate the user's anonymous or pseudo-anonymous identity to third parties. The correspondence between the user's confidential identity (e.g., name, address, financial data) and true identity is unknown within the system during its normal operation. In normal operation a user connects to the system via a client module. The user's confidential identity is masked from a coordination module of the system, which coordination module coordinates tasks necessary to conduct the user's transaction or process the user's communication. A plurality of operating modules are provided to perform tasks such as billing, account management, sending or receiving electronic mail, conducting electronic commerce, etc. In normal operation, no module within the system possesses enough information to determine the user's confidential identity and connect the user to a particular transaction or a particular anonymous or pseudo-anonymous identity. In a monitor mode of operation, however, the content of transactions and communications processed for a particular anonymous or pseudo-anonymous user are recorded or logged pursuant to legal authorization or demand.

WO 00/01108 A3

INTERNATIONAL SEARCH REPORT

Inter onal Application No
PCT/US 99/13908

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10

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 7 G07F

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.
X	US 5 420 926 A (LOW STEVEN H ET AL) 30 May 1995 (1995-05-30)	1-5,21, 22, 25-29, 33,34, 38-42, 58-61,65
A	abstract	6-20,23, 24, 30-32, 35-37, 43-57, 62-64
	column 3, line 9 -column 4, line 28 column 7, line 57 -column 8, line 45 figures 2,5	

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] 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

Date of the actual completion of the international search	Date of mailing of the international search report
3 November 1999	11/11/1999

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	Wolles, B

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/US 99/13908

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 97 25801 A (IBM ;HAUSER RALF CHRISTIAN (CH); TSUDIK GENE (US)) 17 July 1997 (1997-07-17) abstract page 8 -page 10 page 19, line 28 -page 21, line 7	1-65
A	CHAUM D: "SECURITY WITHOUT IDENTIFICATION: TRANSACTION SYSTEMS TO MAKE BIG BROTHER OBSOLETE" COMMUNICATIONS OF THE ASSOCIATION FOR COMPUTING MACHINERY, vol. 28, no. 10, 1 October 1985 (1985-10-01), pages 1030-1044, XP002000086 ISSN: 0001-0782	
A	CHAUM D: "ACHIEVING ELECTRONIC PRIVACY" SCIENTIFIC AMERICAN, vol. 267, no. 2, 1 August 1992 (1992-08-01), pages 76-81, XP000329993 ISSN: 0036-8733	
A	BURK H ET AL: "VALUE EXCHANGE SYSTEMS ENABLING SECURITY AND UNOBSERVABILITY" COMPUTERS & SECURITY INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, vol. 9, no. 8, 1 December 1990 (1990-12-01), pages 715-721, XP000176619 ISSN: 0167-4048	

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte onal Application No
PCT/US 99/13908

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5420926 A	30-05-1995	CA 2134133 A	06-07-1995
		EP 0662673 A	12-07-1995
		JP 7234904 A	05-09-1995
WO 9725801 A	17-07-1997	EP 0876722 A	11-11-1998
		JP 11509354 T	17-08-1999