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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 February 2002 (14.02.2002)

PCT

(10) International Publication Number
WO 02/13445 A3

(51) International Patent Classification[7]: H04L 9/32, G06F 12/14

(21) International Application Number: PCT/US01/24572

(22) International Filing Date: 6 August 2001 (06.08.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/223,076 4 August 2000 (04.08.2000) US

(71) Applicant *(for all designated States except US)*: **FIRST DATA CORPORATION** [US/US]; 6200 South Quebec Street, Suite 330K, Greenwood Village, CO 80111 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **WHEELER, Lynn, Henry** [US/US]; One Canon Drive, Greenwood Village, CO 80111 (US). **WHEELER, Anne, M.** [US/US]; One Canon Drive, Greenwood Village, CO 80111 (US).

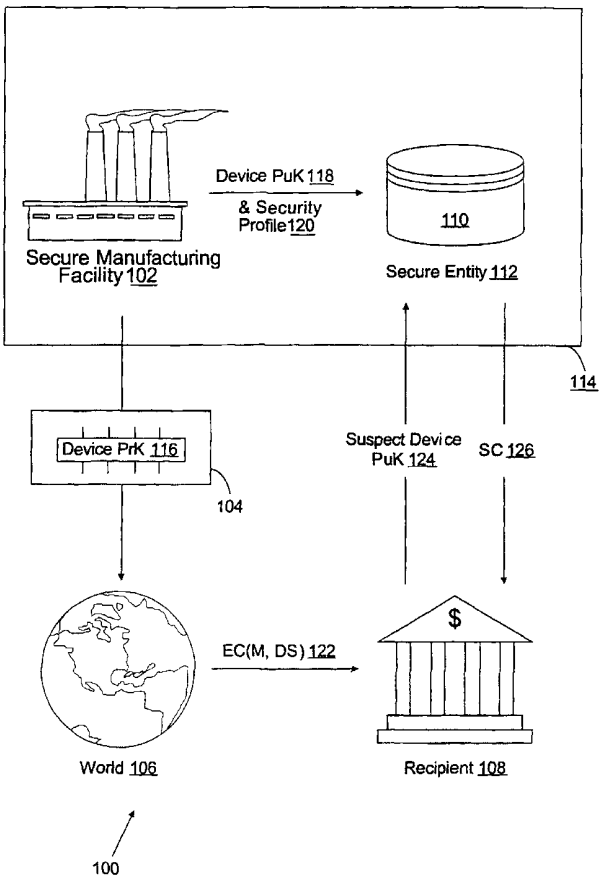
(74) Agents: **TILLMAN, Chad, D.** et al.; Morris, Manning & Martin, LLP, 6000 Fairview Road, Suite 1125, Charlotte, NC 28210 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,

[Continued on next page]

(54) Title: LINKING PUBLIC KEY OF DEVICE TO INFORMATION DURING MANUFACTURE



(57) Abstract: A method in which information pertaining to a device (104) generating digital signatures (122) is reliably identified includes manufacturing (102) devices in a secure environment (114) and for each device (104) before it is released from the secure environment: creating a public-private key pair (116, 118); storing the private key (116) within the device (104) for utilization in generating a digital signature (122) for a message (122); and linking the public key (118) to a Security Profile (120) of the device (104). The devices (104) then are released from the secure environment (114) and a digital signature (122) is received from somewhere (108) in the world (106). The message (122) is authenticated using a suspect public key (124) and the suspect public key (124) is compared with the linked public keys (118). A Security Profile (120) of the genuine device (104) to which belongs the private key (116) used in generating the digital signature (122) is identified when the public key (124) matches a linked public key (118). A risk that the message (122) is fraudulently signed is determined.

WO 02/13445 A3

IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv)) for US only*

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
27 June 2002

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.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/24572

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :H04L 9/32; G06F 12/14
US CL :713/155, 175
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)

U.S. : Please See Extra Sheet.

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

Please See Extra Sheet.

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

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Please See Continuation of Second Sheet.	

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"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
"A"	document defining the general state of the art which is not considered to be of particular relevance	"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
"E"	earlier document published on or after the international filing date	"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
"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)	"&"	document member of the same patent family
"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		

Date of the actual completion of the international search 19 FEBRUARY 2002	Date of mailing of the international search report 15 APR 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Peggy Harvey JUSTIN T. DARROW Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/24572

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,009,177 A (SUDIA) 28 December 1999, col. 12, lines 52-67; col. 13, lines 1-21 and 64-67; col. 14, lines 1-67; col. 15, lines 47-58; col. 17, lines 41-45 and 50-67; col. 18, lines 1-11; col. 20, lines 26-54; col. 28, lines 49-67; col. 29, lines 1-32; col. 33, lines 59-67; col. 34, lines 1-20; figure 15; figure 16; and figure 19, items 192, 194, 195, 196.	1-5, 25/1-3 0/1, 40/2, 40/3, 45/1-47/1,22-24, 25/23, 26/22-30/22, 39/22, 40/22, 45/22-47/22, 73-89, 91
----		----
Y		41/1-44/1,25/6-30/6, 39/6, 40/6, 45/6-47/6,41/22-44/22, 66-72
----		----
A		31/1-38/1,48/1-63/1,31/22-38/22, 48/23-55/23, 31/6-38/6, 90
X	US 5,778,072 A (SAMAR) 7 July 1998, col. 2, lines 52-67; col. 3, lines 63-67; col. 4, lines 1-7 and 28-67; col. 5, lines 1-6 and 47-62; col. 7, lines 2-4 and 61-67; col. 8, lines 1-61; and figure 1, items 101, 123, 125, 127.	6-8, 15/6-1 8/6, 64, 65, 92, 93, 95-100
----		----
Y		13/6, 14/6, 25/6-30/6,39/6-47/6,9-12, 13/12, 14/9-18/9,25/12, 26/9-30/9,39/9, 40/9, 41/12-44/12, 45/9-47/9,66-72, 101-103
----		----
A		19/6-21/6,31/6-38/6,48/6-59/6,19/9-21/9,31/9-38/9,48/12-55/12, 60/9-63/9,94, 104-109
Y	US 5,787,172 A (ARNOLD) 28 July 1998, col. 13, lines 21-38 and 54-67; col. 14, lines 1-9; col. 15, lines 55-64; col. 16, lines 22-28 and 55-67; col. 17, lines 1-17 and 31-36; col. 35, lines 6-28, Appendix A1; figure 3, steps 308, 312; and figure 4A, step 416.	9-12, 13/12, 14/9-18/9, 25/12, 26/9-30/9, 39/9, 40/9, 41/12-44/12, 45/9-47/9
----		----
A		31/1-38/1, 31/6-38/6,19/9-21/9, 31/9-38/9,31/22-38/22, 48/12-55/12, 60/9-63/9, 94

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/24572

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6,021,202 A (ANDERSON et al.) 1 February 2000, col. 25, lines 64-67; col. 26, lines 1-14; col. 33, lines 38-51; col. 38, lines 37-61; col. 39, lines 1-11 and 21-29; and figures 6, 11, 25, 26, and 27.	41/1-44/1,41/6-44/6,41/12-44/12, 41/22-44/22, 102, 103
A	US 5,970,147 A (DAVIS) 19 October 1999, col. 2, lines 40-53.	48/1-63/1,48/6-59/6,48/12-55/12, 60/9-63/9,48/23-55/23

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/24572

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Please See Extra Sheet.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/24572

B. FIELDS SEARCHED
Minimum documentation searched
Classification System: U.S.

IPC(7): G06F 12/14, 17/30, 17/60; H04L 9/12, 9/20, 9/30, 9/32
U.S.: 705/4, 67, 71, 73, 75, 76, 77, 78; 707/201, 202, 203, 204; 380/30, 46, 279, 281, 282; 713/155, 156, 159, 161, 170, 172, 175, 176, 179, 181, 188

B. FIELDS SEARCHED
Documentation other than minimum documentation that are included in the fields searched:

C. Kaufman et al., "Network Security: Private Communication in a Public World," Prentice Hall PTR, 1995.
B. Schneier, "Applied Cryptography Second Edition: Protocols, Algorithms, and Source Code in C," John Wiley & Sons, 1995.

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

EAST(USPAT,EPO,JPO,DERWENT,USPGPUB), DIALOG
search terms: device, computer, client, host, terminal, settop, box, PDA, handheld, telephone, smartcard, token, public key, open key, secret key, private key, sign, signature, encrypt, encipher, scramble, verify, authenticate, confirm, decrypt, decipher, unscramble, security detail, feature, profile, record, manufacture, construct, fabricate, originate, guarantee, waranty, insurance, database, directory, administrator, authorize, center, user, customer, subscriber, receiver, recipient, member

BOX II. OBSERVATIONS WHERE UNITY OF INVENTION WAS LACKING
This ISA found multiple inventions as follows:

This application contains the following inventions or groups of inventions which are not so linked as to form a single inventive concept under PCT Rule 13.1. In order for all inventions to be searched, the appropriate additional search fees must be paid.

Group I, claims 1-5, 25/1-38/1, 40/2, 40/3, and 41/1-63/1; 22-24, 25/23, 26/22-47/22, and 48/23-54/23; 73-83; and 84-91, drawn to a method in which information of a device that generates digital signatures is reliably identified, a method of providing for reliably identifying a Security Profile of a device that generates digital signatures, a method of establishing an initial PuK-linked account database record of a user with each one of a plurality of third-parties, and a method of manufacturing devices that generate digital signatures such that each device may be reliably and uniquely identified, respectively.
Group II, claims 6-8, 19/6-21/6, and 25/6-59/6; 9-12, 13/12, 14/9-21/9, 25/12, 26/9-40/9, 41/12-44/12, 45/9-47/9, 48/12-55/12, and 60/9-63/9; 64-72; and 92-109, drawn to one method of managing a database for reliably identifying a Security Profile of a device that generates digital signatures, another method of managing a database for reliably identifying a Security Profile of a device that generates digital signatures, a method of establishing an initial PuK-linked account database, and a method of maintaining a Central Key Authority (CKA) database, respectively.

The inventions listed as Groups I and II do not relate to a single inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: the special technical feature of the Group I invention is creating or obtaining a public-private key pair and linking the public key with other information associated with a device that generates digital signatures while the special technical feature of the Group II invention is maintaining a database with the public key in association with a security profile of each device that generates digital signatures. Since the special technical feature of the Group I invention is not present in the Group II invention being claimed, unity of invention is lacking.