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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 February 2003 (20.02.2003)

PCT

(10) International Publication Number
WO 03/015370 A3

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number: PCT/GB02/03707

(22) International Filing Date: 12 August 2002 (12.08.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0119629.4 10 August 2001 (10.08.2001) GB

(71) Applicant *(for all designated States except US)*: **CRYPTOMATHIC A/S** [DK/DK]; Kannikegade 14, 3, DK-8000 Aarhus C (DK).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **LANDROCK, Peter** [DK/GB]; 52 Storey's Way, Cambridge, Gambridgeshire CB3 0DX (GB). **TULIANI, Jonathan, Roshan** [GB/GB]; 206 The Rowans, Milton, Cambridge, Cambridgeshire CB4 6ZL (GB).

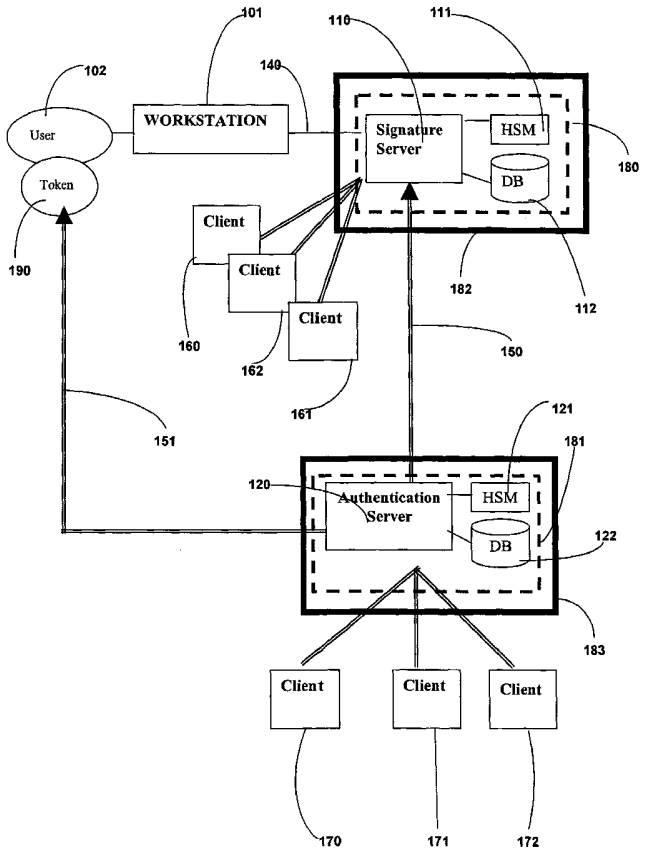
(74) Agent: **MOUNTENEY, Simon, James**; Marks & Clerk, 57-60 Lincolns Inn Fields, London WC2A 3LS (GB).

(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, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),

[Continued on next page]

(54) Title: DATA CERTIFICATION METHOD AND APPARATUS



(57) Abstract: An apparatus and method for signing electronic data with a digital signature in which a central server comprises a signature server (110) and a authentication server (120). The signature server (110) securely stores the private cryptographic keys of a number of users (102). The user (102) contacts the central server using a workstation (101) through a secure tunnel which is set up for the purpose. The user (102) supplies a password or other token (190), based on information previously supplied to the user by the authentication server (120) through a separate authentication channel. The authentication server provides the signature server with a derived version of the same information through a permanent secure tunnel between the servers, which is compared with the one supplied by the user (102). If they match, data received from the user (102) is signed with the user's private key.

WO 03/015370 A3

Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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:
24 April 2003

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/GB 02/03707

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

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 H04L G06F

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)
EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	TORBEN PEDERSEN: "Signature Server" NEWSONINK, 'Online! January 2001 (2001-01), XP002215192 Retrieved from the Internet: <URL:http://www.cryptomathic.com/pdf/news5 .pdf> 'retrieved on 2002-09-27!	1-14, 16-24, 32-38, 43,44, 47-53, 63,66-70
Y	page 4	25-28, 42, 54-59,74

A	CRYPTOMATHIC: "Home Page" CRYPTOMATHIC WEB SITE, 'Online! 18 May 2001 (2001-05-18), XP002215194 Retrieved from the Internet: <URL:http://web.archive.org/web/2001051817 0810/http://www.cryptomathic.com/> 'retrieved on 2002-09-30! New Approach to Digital Signatures	1-38,43, 44,47-70

	-/--	

[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
10 February 2003	07.03.03

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	Bertolissi, E

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

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 02/03707

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	CRYPTHOMATIC: "EasySign - A User-friendly Way of doing Mobile Commerce" CRYPTHOMATIC WEB SITE, 'Online! 6 August 2001 (2001-08-06), XP002215193 Retrieved from the Internet: <URL:http://web.archive.org/web/20010806151906/http://www.cryptomathic.com/products/easysign.html> 'retrieved on 2002-09-30! the whole document	1-38,43, 44,47-70
A	CRYPTOMATHIC: "A NEW APPROACH TO DIGITAL SIGNATURES" CRYPTOMATHIC WEB SITE, 'Online! 1 August 2001 (2001-08-01), XP002215195 Retrieved from the Internet: <URL:http://web.archive.org/web/20010801150532/http://www.cryptomathic.com/news/tech_frame_sigserv.html> 'retrieved on 2002-09-30! the whole document	1-38,43, 44,47-70
Y	GARFINKEL SIMSON ET AL: "Web Security & Commerce" WEB SECURITY AND COMMERCE, XX, XX, June 1997 (1997-06), pages 108-111, XP002182557 page 108	25,28, 54,59
A	HOLLOWAY C J: "Controlling Digital Signature Services Using A Smartcard" COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, NL, vol. 14, no. 8, 1995, pages 681-690, XP004000216 ISSN: 0167-4048 Introduction	1-38,43, 44,47-70
Y	US 6 078 908 A (SCHMITZ KIM) 20 June 2000 (2000-06-20) abstract column 6, line 55 -column 7, line 30 column 1, line 45 -column 4, line 9	26,27, 55-58
X	US 6 058 480 A (BROWN GARY S) 2 May 2000 (2000-05-02)	39-41, 45,46, 71-73
Y	abstract column 6, line 52 - line 67 column 8, line 40 -column 10, line 9 column 11, line 28 - line 42 figure 2	42,74

-/--

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 02/03707

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 668 876 A (FALK JOHAN PER ET AL) 16 September 1997 (1997-09-16) abstract column 6, line 58 -column 9, line 12 figure 1A	39-42, 45,46, 71-74
A	WO 01 17310 A (ERICSSON TELEFON AB L M) 8 March 2001 (2001-03-08) abstract page 11, line 8 -page 12, line 22 figure 3	39-42, 45,46, 71-74

INTERNATIONAL SEARCH REPORT

International application No.
PCT/GB 02/03707

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

This International Search 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:

see additional 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.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-38, 43, 44, 47-70

   Method, computer apparatus, carrier method and data certifying apparatus for certifying electronic data

2. Claims: 39-42, 45, 46, 71-74

   Method, computer apparatus, carrier method and an apparatus for supplying user identification data

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 02/03707

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6078908 A	20-06-2000	DE 19718103 A1	04-06-1998
		AT 226346 T	15-11-2002
		AU 6354598 A	05-11-1998
		BR 9801177 A	20-03-2001
		CN 1207533 A	10-02-1999
		DE 59805939 D1	21-11-2002
		EP 0875871 A2	04-11-1998
		JP 10341224 A	22-12-1998
		TW 425804 B	11-03-2001
US 6058480 A	02-05-2000	US 5740361 A	14-04-1998
		US 6487667 B1	26-11-2002
US 5668876 A	16-09-1997	AU 692881 B2	18-06-1998
		AU 2688795 A	19-01-1996
		CA 2193819 A1	04-01-1996
		CN 1156531 A ,B	06-08-1997
		EP 0766902 A2	09-04-1997
		FI 965161 A	13-02-1997
		JP 10502195 T	24-02-1998
		WO 9600485 A2	04-01-1996
WO 0117310 A	08-03-2001	AU 7047100 A	26-03-2001
		CN 1385051 T	11-12-2002
		EP 1208715 A1	29-05-2002
		WO 0117310 A1	08-03-2001