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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 May 2009 (14.05.2009)

PCT

(10) International Publication Number
WO 2009/059569 A3

(51) International Patent Classification:
G06F 21/04 (2006.01) *G06F 21/24* (2006.01)

(21) International Application Number:
PCT/CZ2008/000131

(22) International Filing Date: 24 October 2008 (24.10.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PV 2007-779 8 November 2007 (08.11.2007) CZ

(71) Applicant *(for all designated States except US)*: **MONET+, A.S.** [CZ/CZ]; Za Dvorem 505, 763 14 Zlin, Stipa (CZ).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **ENDRYS, Bretislav** [CZ/CZ]; Lesni ctvrt 1/3541, 760 01 Zlin (CZ).

(74) Agents: **ANDERA, Jiri** et al.; Rott, Ruzicka & Guttmann, P.O. Box 94, 170 00 Praha 7 (CZ).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (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))*

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:
25 June 2009

(54) Title: METHOD FOR SECURING AUTHORIZED DATA ENTRY AND THE DEVICE TO PERFORM THIS METHOD

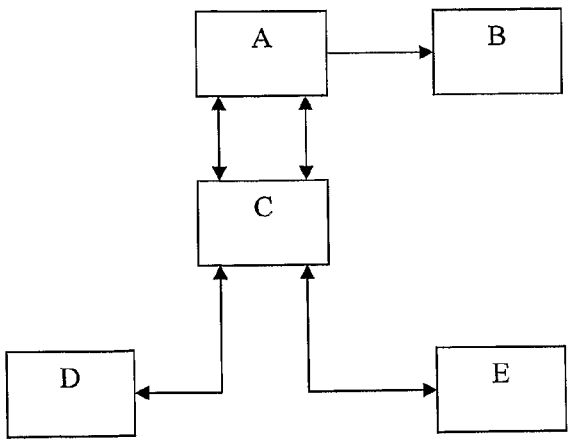

Fig. 1

(57) Abstract: The method for authorized data entry and securing the authenticity of such data when entering cryptographic operations is characterised in that the application in the computer (A), requiring authorized data entry, sends a specific command to the STM module (C) which defines a template of input data intended to be cryptographically processed. This specific command switches the STM module (C) over to the secure typing mode, the STM module (C) autonomously controls the typing of required data items of the data template, by recording characters typed on the connected entry device (D) and the recorded characters are arranged by the STM module (C) in its internal memory in requested data structures defined by the the input data template, and such created data are sent by the STM module (C) directly to the token (E) where the requested cryptographic operation is called, the result of which is sent to the computer (A) by the STM module (C), and subsequently the STM module (C) switches back to the transparent mode. For the devices according to the present invention, both the data entry device (D) and the external token (E) are connected to the computer (A) via an additional STM module (C) which is standardly in the transparent mode when transferring data between the computer (A) and connected peripherals, such as the data entry device (D) and the token (E), without affecting the process, with the specific command sent from the appliction in the computer (A) being a transferrable template of data defining the requirements for the input data of cryptographic operations and the STM module (C) which can be switched over to the secure typing mode where the STM module (C) autonomously controls data typing on the data entry device (D) and their cryptographic processing in the token (E).

WO 2009/059569 A3

INTERNATIONAL SEARCH REPORT

International application No
PCT/CZ2008/000131

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/04 G06F21/24

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)
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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	EP 1 632 838 A (O2 MICRO INTERNAT LTD [KY]) 8 March 2006 (2006-03-08) paragraphs [0009] - [0014], [0024], [0025], [0037], [0040], [0046] - [0049]; figures 2,4	1-4,6-9 5
Y	GB 2 267 986 A (ALGORITHMIC RES LTD [IL]) 22 December 1993 (1993-12-22) page 1, line 11 - page 2, line 37 page 3, line 33 - page 4, line 24 page 5, line 33 - page 6, line 6 page 7, line 29 - page 8, line 8 page 8, line 34 - page 9, line 15	1-4,6-9
Y	EP 0 763 791 A (HEWLETT PACKARD CO [US]) 19 March 1997 (1997-03-19) column 8, line 10 - line 23 column 2, line 50 - column 4, line 9	4

-/--

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

[X] See patent family 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
21 April 2009	07/05/2009

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, Fax: (+31-70) 340-3016	Veillas, Erik

INTERNATIONAL SEARCH REPORT

International application No
PCT/CZ2008/000131

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 10 2005 008433 A1 (GIESECKE & DEVRIENT GMBH [DE]) 31 August 2006 (2006-08-31) the whole document	1-9
A	US 4 405 829 A (RIVEST RONALD L [US] ET AL) 20 September 1983 (1983-09-20) the whole document	1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/CZ2008/000131

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1632838 A	08-03-2006	NONE	
GB 2267986 A	22-12-1993	DE 69333122 D1	04-09-2003
		DE 69333122 T2	15-04-2004
		EP 0587375 A2	16-03-1994
		IL 103062 A	04-08-1996
		SG 43927 A1	14-11-1997
		US 5406624 A	11-04-1995
EP 0763791 A	19-03-1997	US 5920730 A	06-07-1999
DE 102005008433 A1	31-08-2006	WO 2006089710 A1	31-08-2006
US 4405829 A	20-09-1983	NONE	