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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 June 2007 (07.06.2007)

PCT

(10) International Publication Number
WO 2007/062941 A3

(51) International Patent Classification:
G06F 21/00 (2006.01) *G06F 12/14* (2006.01)

(21) International Application Number:
PCT/EP2006/067807

(22) International Filing Date: 26 October 2006 (26.10.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/275,015 1 December 2005 (01.12.2005) US

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET LM ERICSSON (publ)** [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BLOM, Rolf** [SE/SE]; Svärdvägen 2, S-175 68 Järfälla (SE). **GEHRMANN, Christian** [SE/SE]; Skördevägen 2c, S-227 38 Lund (SE).

(74) Agents: **BRATT, Hanna** et al.; Nya Vattentornet, S-221 83 Lund (SE).

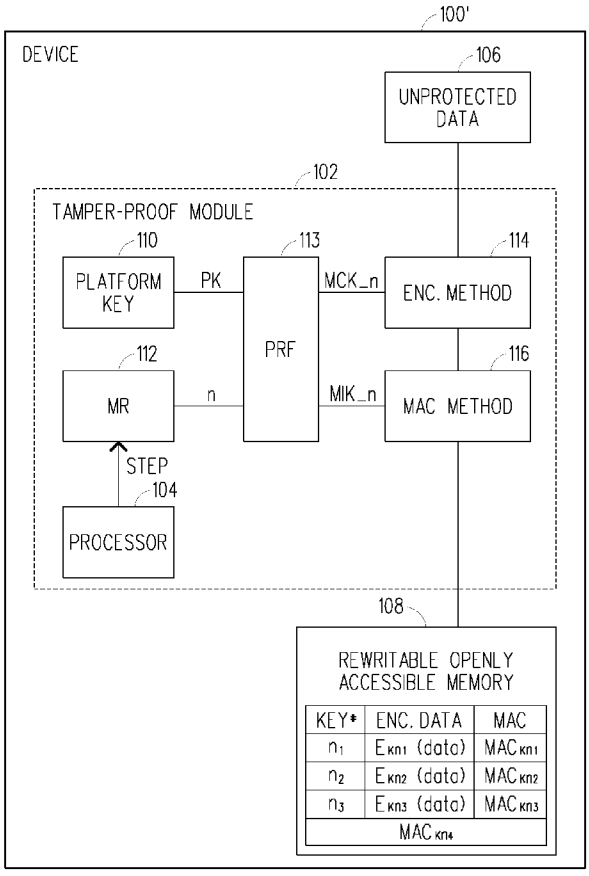
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, 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, 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, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) **Title:** SECURE AND REPLAY PROTECTED MEMORY STORAGE



(57) **Abstract:** A device (e.g., mobile device) and method are described herein that can protect data stored in a rewritable openly accessible memory from replay attacks by using an integrity key and an encryption key to en/decrypt the data, integrity protect the data via a MAC calculation, and verify the data.

WO 2007/062941 A3

— *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:
26 July 2007

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/EP2006/067807

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00 G06F12/14

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, 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	US 5 757 919 A (HERBERT HOWARD C [US] ET AL) 26 May 1998 (1998-05-26) column 1, line 58 - column 2, line 5 column 2, line 25 - column 3, line 8 column 4, lines 15-42 column 7, lines 15-51	1-23
A	WO 01/33317 A (KONINKL PHILIPS ELECTRONICS NV [NL]) 10 May 2001 (2001-05-10) pages 1-3; figures 1-3	

-/--

[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
25 May 2007	05/06/2007

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	Preuss, Norbert

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2006/067807

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 02/27441 A (ERICSSON TELEFON AB L M [SE]; SMEETS BEN [SE]) 4 April 2002 (2002-04-04) page 2, line 10 - page 3, line 7 page 7, lines 13-26 page 8, line 8 - page 9, line 15 page 9, line 25 - page 11, line 27 page 14, line 26 - page 18, line 19	
A	US 2004/193888 A1 (WISEMAN WILLARD M [US] ET AL) 30 September 2004 (2004-09-30) page 29, lines 1-7 page 7, paragraph 5.1	
A	US 2003/194094 A1 (LAMPSON BUTLER W [US] ET AL) 16 October 2003 (2003-10-16) paragraphs [0133] - [0135] paragraphs [0010] - [0004] figures 4,5	
A	SCHNEIER B: "Applied cryptography, second edition: protocols, algorithms, and source code in C" APPLIED CRYPTOGRAPHY : PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C, NEW YORK, NY : JOHN WILEY & SONS, US, 1996, pages 28-29,169, XP002985121 ISBN: 0-471-12845-7 pages 29,175	
A	LAMPORT L: "PASSWORD AUTHENTICATION WITH INSECURE COMMUNICATION" COMMUNICATIONS OF THE ASSOCIATION FOR COMPUTING MACHINERY, ACM, NEW YORK, NY, US, vol. 24, no. 11, 1 November 1981 (1981-11-01), pages 770-772, XP000577349 ISSN: 0001-0782 pages 770-771	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2006/067807

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5757919 A	26-05-1998	AU 5688998 A	03-07-1998
		DE 19782169 C2	06-09-2001
		DE 19782169 T0	28-10-1999
		GB 2334866 A	01-09-1999
		HK 1022797 A1	22-03-2002
		JP 2001508893 T	03-07-2001
		WO 9826535 A1	18-06-1998
WO 0133317 A	10-05-2001	EP 1141808 A1	10-10-2001
		JP 2003513388 T	08-04-2003
WO 0227441 A	04-04-2002	AT 355551 T	15-03-2006
		AU 1227902 A	08-04-2002
		CN 1466710 A	07-01-2004
		EP 1325401 A1	09-07-2003
		US 2002038429 A1	28-03-2002
US 2004193888 A1	30-09-2004	NONE	
US 2003194094 A1	16-10-2003	US 2006021064 A1	26-01-2006
		US 7194092 B1	20-03-2007
		US 2003196085 A1	16-10-2003
		US 2003196099 A1	16-10-2003
		US 2003196110 A1	16-10-2003