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

## (19) World Intellectual Property Organization

International Bureau



# 

(43) International Publication Date 26 October 2006 (26.10.2006)

PCT

# (10) International Publication Number WO 2006/113241 A3

(51) International Patent Classification: *H04K 1/00* (2006.01) *H04L 9/00* (2006.01)

(21) International Application Number:

PCT/US2006/013549

(22) International Filing Date: 11 April 2006 (11.04.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

11/105,065 13 April 2005 (13.04.2005) US

(71) Applicant (for all designated States except US): HEWLETT-PACKARD DEVELOPMENT COM-PANY, L. P. [US/US]; 20555 S. H. 249, Houston, Texas 77070 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): PRADHAN, Salil [IN/US]; 1501 Page Mill Road, Palo Alto, California 94304 (US). DEOLALIKAR, Vinay [IN/US]; 1501 Page Mill Road, Palo Alto, California 94304 (US). ORTIZ.

Lester [US/US]; Highway 110 N Km 5.1, Aguadilla, 00605 (PR). CABAN, Alipio [US/US]; Highway 110 N Km 5.1, Aguadilla, 00605 (PR). LYON, Geoff, M. [GB/US]; 1501 Page Mill Road, Palo Alto, California 94304 (US).

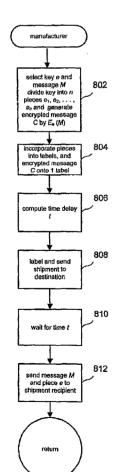
(74) Agent: LEE, Denise, A.; Hewlett-Packard Company, Intellectual Property Administration, P O Box 272400, M/S 35, Fort Collins, Colorado 80524-2400 (US).

(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, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH,

[Continued on next page]

#### (54) Title: METHOD AND SYSTEM FOR SHIPMENT AUTHENTICATION



(57) Abstract: In one embodiment of the present invention, a source point of a supply chain secures shipment of an object by devising an encryption key (604) and encrypting a message (610) using the encryption key to produce an encrypted message (612). A portion (606) or portions of the encryption key and the encrypted message are included or incorporated (614) within the object to be shipped, packaging surrounding the object, and/or labels (608) affixed to the object or packaging (602), prior to shipping the object to a destination point within the supply chain. Upon receipt of the object from the supply chain, the destination point can extract (902) the portion or portions of the encryption key and the encrypted message from the object, packaging surrounding the object, and/or labels affixed to the object or packaging, obtain (904) the remaing portion of the encryption key directly from the source point, reassemble (907) the encryption key, and decrypt the encrypted message to produce a computed message. The destination point can then obtain the original message from the source point and compare (908) the original message to the decrypted message in order to determine whether or not the shipment is authentic.

### WO 2006/113241 A3



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

- 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 April 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/US06/13549

A. CLASSIFICATION OF SUBJECT MATTER  IPC: H04K 1/00( 2007.01);H04L 9/00( 2007.01)				
USPC: 380/28;380/30;3 80/44 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.: 380/28; 380/30;3 80/44				
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 practicable, search terms used) EAST SEARCH, PLUS SEARCH				
C. DOC	UMENTS CONSIDERED TO BE RELEVANT			
Category *	Citation of document, with indication, where appropriate, of the relevant passages			Relevant to claim No.
Y	US Publication 2004/0208316 A1 (Wack et al.) 21 October 2004 (21.10.2004), Figures 1-5,			1-10
Y	paragraph 0003-0110. US 5,588,061 A (GANESAN et al.) 24 December 1996 (24.12.1996), Abstract, Figures 2-4, Column 1, line 20 - Column 9, line 20.			1-10
Further	documents are listed in the continuation of Box C.	Se	e patent family annex.	
* S	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  "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	
"A" document defining the general state of the art which is not considered to be of particular relevance		pr		
•	earlier application or patent published on or after the international filing date			
establish	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 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	
"O" document	t referring to an oral disclosure, use, exhibition or other means	ol	obvious to a person skilled in the art	
	t published prior to the international filing date but later than the ate claimed	"&" document member of the same patent family		
Date of the actual completion of the international search 27 November 2006 (27.11.2006)		Date of mailing of the international search report		
Name and mailing address of the ISA/US		Authorized	Authorized officer	
Mail Stop PCT, Attn: ISA/US Commissioner for Patents		Authorized officer Baotran N. To for Modwelle & Exm		
P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201		Telephone No. 571-272-8156		

Form PCT/ISA/210 (second sheet) (April 2005)