

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
11 May 2006 (11.05.2006)

PCT

(10) International Publication Number
WO 2006/049832 A3

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

(21) International Application Number:
PCT/US2005/036749

(22) International Filing Date: 12 October 2005 (12.10.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/980,393 2 November 2004 (02.11.2004) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:

US 10/980,393 (CIP)
Filed on 2 November 2004 (02.11.2004)

(71) Applicant (for all designated States except US): **VOLTAGE SECURITY, INC.** [US/US]; 1070 Arastradero Road, Suite 100, Palo Alto, CA 94304 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **APPENZELLER,**

Guido [DE/US]; 1035 Noel Drive, Apt. F, Menlo Park, CA 94025 (US). **SPIES, Terence** [US/US]; 826 Wharfside Road, San Mateo, CA 94404 (US). **BOYEN, Xavier** [BE/US]; 2721 Midtown Ct.315, Palo Alto, CA 94303 (US).

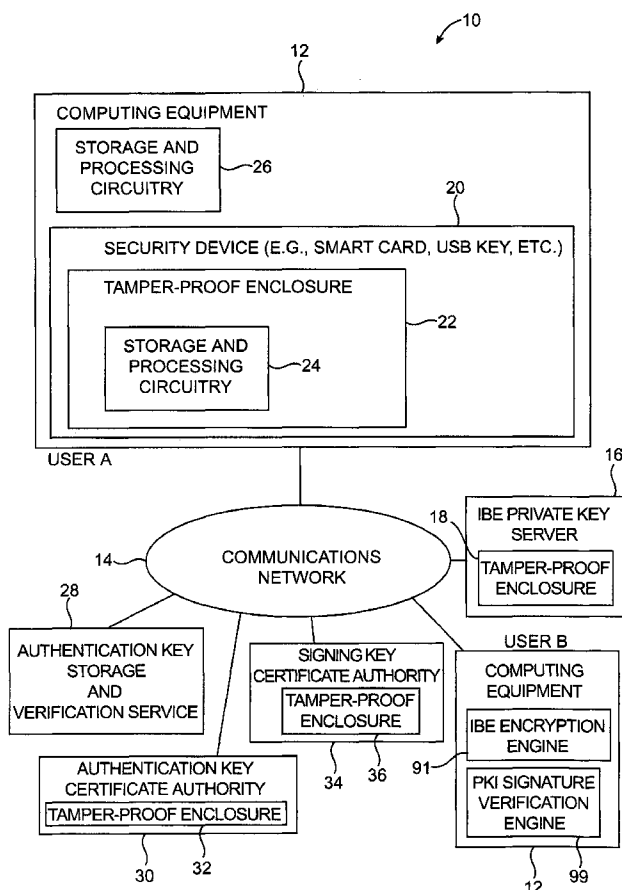
(74) Agent: **TREYZ, Victor, G.**; 870 Market Street, Suite 984, San Francisco, CA 94102 (US).

(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, 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 (patent), UZ, VC, VN, YU, 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,

[Continued on next page]

(54) Title: SECURITY DEVICE FOR CRYPTOGRAPHIC COMMUNICATIONS



(57) Abstract: Cryptographic systems and methods are provided in which authentication operations, digital signature operations, and encryption operations may be performed. Authentication operations may be performed using authentication information. The authentication information may be constructed using a symmetric authentication key or a public/private pair of authentication keys. Users may digitally sign data using private signing keys. Corresponding public signing keys may be used to verify user signatures. Identity-based-encryption (IBE) arrangements may be used for encrypting messages using the identity of a recipient. IBE-encrypted messages may be decrypted using appropriate IBE private keys. A smart card, universal serial bus key, or other security device having a tamper-proof enclosure (Figure 1, 20) may use the authentication information to obtain secret key information. Information such as IBE private key information, private signature key information, and authentication information may be stored in the tamper-proof enclosure.



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:
1 February 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/US05/36749

A. CLASSIFICATION OF SUBJECT MATTER

IPC: H04L 9/00(2006.01)

USPC: 713/171

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. : 713/171

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	USPGPUB 2003/0081785 A1 (Boneh et al) 1 May 2003 (01.05.2003), page 5, pp 64; page 9, pp 123-127; page 15, pp 263page 17, pp 299	1-20
Y	USPGPUB 2004/0172531 A1 (Little et al) 02 September 2004 (02.09.2004), page 3, pp 36, page 4, pp 43-45, page 8, pp 82.	1-20
Y	US 6,792,536 B1 (Teppler) 14 September 2004 (14.09.2004), column 32, line 47-column 33, line 33.	10-20

☐ Further documents are listed in the continuation of Box C.

☐ 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 application or patent 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

06 October 2006 (06.10.2006)

Date of mailing of the international search report

30 NOV 2006

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Facsimile No. (571) 273-3201

Authorized officer

Emmanuel Moise

Telephone No. 571-272-2100