(20060241297)
11.04.06

162162

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 June 2005 (30.06.2005)

PCT

(10) International Publication Number
WO 2005/060151 A3

(51) International Patent Classification[7]: H04L 9/08

(21) International Application Number:
PCT/US2004/041909

(22) International Filing Date:
13 December 2004 (13.12.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/528,890 11 December 2003 (11.12.2003) US
10/815,454 31 March 2004 (31.03.2004) US

(71) Applicant *(for all designated States except US)*: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **WHEELER, David** [US/US]; 516 East Jasper Drive, Gilbert, AZ 85296 (US). **BRIZEK, John** [US/US]; 3050 Marci Lane, Placerville, CA 95667 (US). **KHAN, Moinul** [BD/US]; 10842 Redmond Road, Austin, TX 78739 (US). **KONA, Anitha** [IN/US]; 3413 Normandy Ridge Lane, Austin, TX 78738 (US).

(74) Agents: **STEFFEY, Charles, E.** et al.; Schwegman, Lundberg, Woessner & Kluth, P.A., P.O. Box 2938, Minneapolis, MN 55402 (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, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

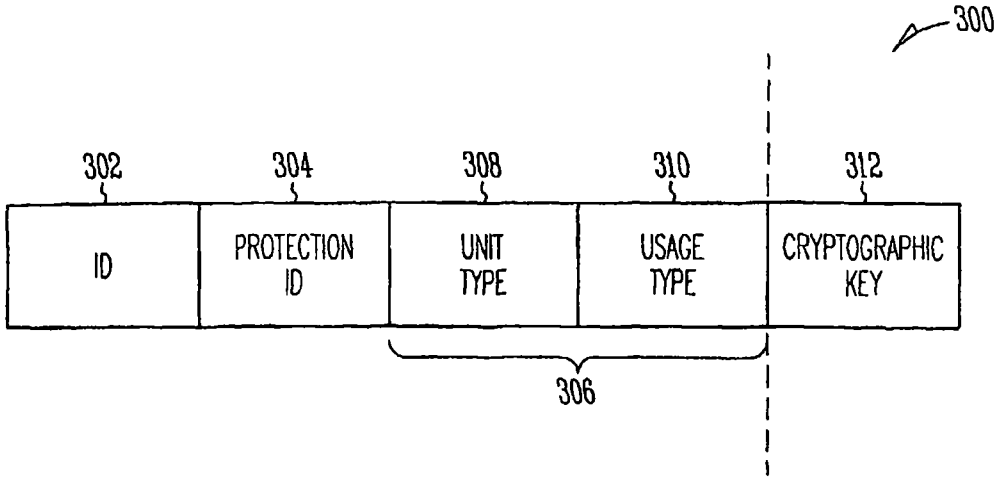
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, 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*

(88) Date of publication of the international search report:
6 October 2005

[Continued on next page]

(54) Title: TRUSTED MOBILE PLATFORM ARCHITECTURE



(57) Abstract: In an embodiment, an apparatus includes one or more cryptographic units. The apparatus also includes a memory to store one or more data encryption keys and an associated header for the one or more data encryption keys. The associated header defines which of the one or more cryptographic units are to use the data encryption key.

WO 2005/060151 A3

ACTION

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.