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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 December 2006 (21.12.2006)

PCT

(10) International Publication Number
WO 2006/133545 A1

(51) International Patent Classification:
H04L 9/00 (2006.01) *H04L 9/28* (2006.01)

(21) International Application Number:
PCT/CA2006/000944

(22) International Filing Date: 12 June 2006 (12.06.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/690,155	14 June 2005 (14.06.2005)	US
2,510,366	21 June 2005 (21.06.2005)	CA
60/777,262	28 February 2006 (28.02.2006)	US
2,538,087	28 February 2006 (28.02.2006)	CA

(71) Applicant *(for all designated States except US)*: **CERTICOM CORP.** [CA/CA]; 5520 Explorer Drive, 4th Floor, Mississauga, Ontario L4W 5L1 (CA).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **NEILL, Brian** [CA/CA]; 2135 Donald Road, Burlington, Ontario L7M 3R3 (CA). **VADEKAR, Ashok** [CA/CA]; R.R. #4, 250 Harris Street, Rockwood, Ontario N0B 2K0 (CA). **XU, Patrick** [CA/CA]; 21 Greyfriars Avenue, Richmond Hill, Ontario L4E 4R4 (CA). **WALTERS, Anthony, J.** [CA/CA]; 57 Sanderson Cr, Richmond Hill, Ontario L4C 5L5 (CA). **ROSATI, Tony** [CA/CA]; 167 Grandview Road, Ottawa, Ontario K2H 8B8 (CA).

(74) Agents: **SLANEY, Brett, J.** et al.; Blake, Cassels & Graydon LLP, 199 Bay Street, Suite 2800, Box 25, Commerce Court West, Toronto, Ontario M5L 1A9 (CA).

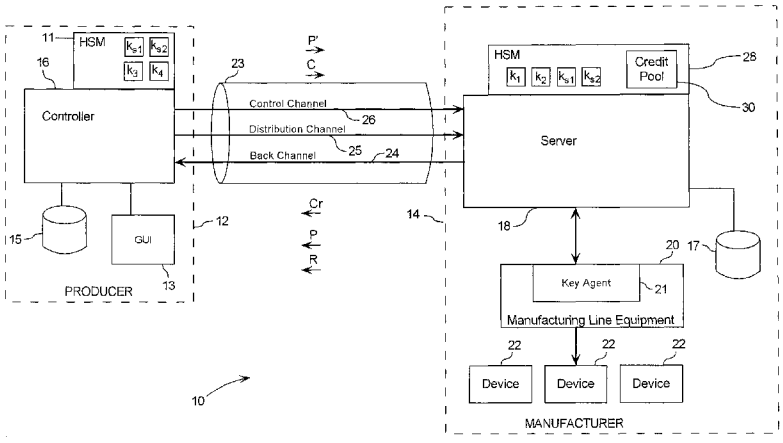
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, 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, 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: SYSTEM AND METHOD FOR REMOTE DEVICE REGISTRATION



(57) Abstract: A system and method for remote device registration, to monitor and meter the injection of keying or other confidential information onto a device, is provided. A producer who utilizes one or more separate manufacturers, operates a remote module that communicates over forward and backward channels with a local module at the manufacturer. Encrypted data transmissions are sent by producer to the manufacturer and are decrypted to obtain sensitive data used in the devices. As data transmissions are decrypted, credits from a credit pool are depleted and can be replenished by the producer through credit instructions. As distribution images are decrypted, usage records are created and eventually concatenated, and sent as usage reports back to the producer, to enable the producer to monitor and meter production at the manufacturer. In an alternative arrangement overproduction may be inhibited by introducing a separation of duties within a manufacturing process. Typically a producer will contract out the various stages of manufacturing to multiple contractors. In general, separation of duties involves purposefully separating manufacturing stages, for silicon chips or other devices, so that the end product must have been "touched", by each subcontractor, in order for the end product to be fully functional.

WO 2006/133545 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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.