IPOS PA1 2000/1670-9

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00 — A1

(11) International Publication Number: **WO 99/17495**

(43) International Publication Date: 8 April 1999 (08.04.99)

(21) International Application Number: PCT/US98/13096

(22) International Filing Date: 24 June 1998 (24.06.98)

(30) Priority Data:
08/938,491 30 September 1997 (30.09.97) US

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

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: DAVIS, Derek, L. [US/US]; 4509 East Desert Trumpet Road, Phoenix, AZ 85044 (US).

(74) Agents: TAYLOR, Edwin, H. et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

(81) Designated States: AL, AM, AT, AT (Utility model), AU (Petty patent), AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: A CIRCUIT AND METHOD FOR CONFIGURING AND REGISTERING A CRYPTOGRAPHIC DEVICE

(57) Abstract

A system and method for configuring and registering a cryptographic device (150). The configuraion phase involves loading a device serial number (DSER) and a symetric key (SK) into non–volatile memory (215) of the cryptographic device (150). The non–volatile memory (215) is integrated with the processing logic (210) of the cryptographic device (150). DSER is provided by an external source while SK is generated within the cryptographic device (150). The registration phase involves providing DSER to a database (415, 420) that contains cryptographic information associated with each cryptographic device (150) manufactured. The cryptographic information includes at least a public key and a private key encrypted with the SK. DSER is ured to locate the appropriate cryptographic information and to transmit the cryptographic information to an electronic system having the cryptographic device (150).

