**PCT** WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32 — A1

(11) International Publication Number: **WO 00/35143**

(43) International Publication Date: 15 June 2000 (15.06.00)

(21) International Application Number: PCT/AU99/01076

(22) International Filing Date: 3 December 1999 (03.12.99)

(30) Priority Data:
PP 7523 4 December 1998 (04.12.98) AU

(71) Applicant *(for all designated States except US)*: VIRTUAL BUSINESS ASSOCIATES PTY. LTD. [AU/AU]; 27 Werona Avenue, Killara, NSW 2046 (AU).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: COLLINS, Lyal, Sidney [AU/AU]; 1/37 Walton Crescent, Abbotsford, NSW 2046 (AU).

(74) Agent: SPRUSON & FERGUSON; G.P.O. Box 3898, Sydney, NSW 2001 (AU).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, 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, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, 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, GW, ML, MR, NE, SN, TD, TG).

**Published**
*With international search report.*

(54) Title: MESSAGE IDENTIFICATION WITH CONFIDENTIALITY, INTEGRITY, AND SOURCE AUTHENTICATION

(57) Abstract

A method for transmitting and receiving a secure message. Transmission is by generating, using a device identifier (408), an application identifier (406) and an application value (412), of a message value (502), combining the message value (502) with one or more first secret values (400), said secret values (400) being known substantially only to the originating device and one or more intended recipient devices of the message, to establish a secret message value (506), applying the secret message value (506) and the message to an encoding process (602) to form a secure message block (604), and combining an address (616, 618) with a device identifier (408), the application identifier (406), the application value (412) and the secure message block (604), to form a secure message (606) for transmission which is decodable by the one or more of said intended recipient devices which thereby recover the message, the address, the device identifier, the application identifier and the application value.

