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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 December 2005 (08.12.2005)

PCT

(10) International Publication Number
WO 2005/117331 A1

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

(21) International Application Number: PCT/GB2005/001479

(22) International Filing Date: 18 April 2005 (18.04.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0411560.6 24 May 2004 (24.05.2004) GB

(71) Applicant *(for all designated States except US)*: **PROTX GROUP LIMITED** [GB/GB]; 6th Floor, 22 Soho Square, London W1D 4NS (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **ALCULUMBRE, Michael** [GB/GB]; 6th Floor, 22 Soho Square, London W1D 4NS (GB).

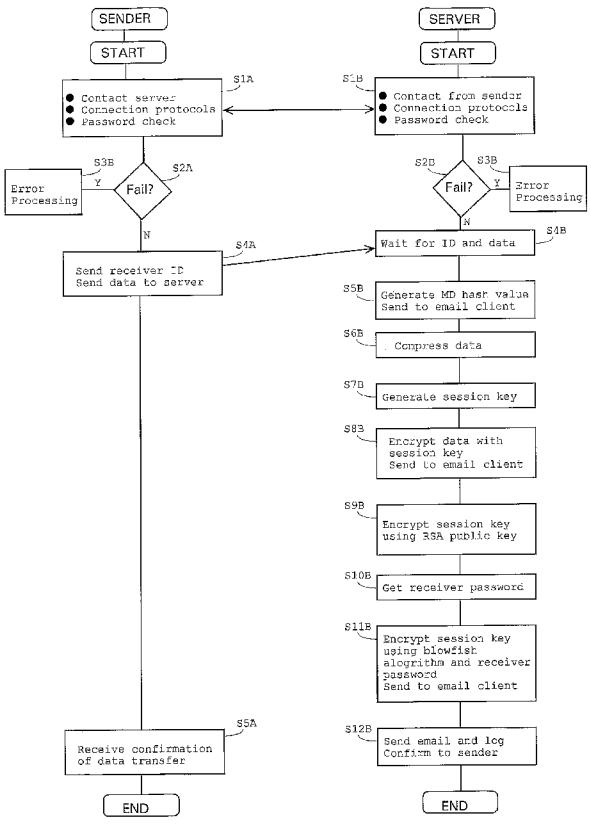
(74) Agents: **ABLETT, Graham, Keith** et al.; Ablett & Stebbing, Caparo House, 101-103 Baker Street, London W1U 6FQ (GB).

(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, 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, 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,

[Continued on next page]

(54) Title: A METHOD OF ENCRYPTING AND TRANSFERRING DATA BETWEEN A SENDER AND A RECEIVER USING A NETWORK



(57) Abstract: The present invention relates to a method of encrypting and transferring data between a sender and a receiver using a network thereby transferring data in a secure manner. The method comprises the steps of a server receiving from the sender an identifier of the receiver (S4A, S4B); establishing a transfer specific encryption key specific to the transfer (S7B); encrypting the data using the transfer specific encryption key (s8B); the server accessing receiver specific information according to the received identifier of the receiver and encrypting, with the receiver specific information, said transfer specific encryption key (S11B); transferring the encrypted data and the encrypted transfer specific encryption key over the network for receipt by the receiver (S11B); the server receiving from the receiver the encrypted transfer specific encryption key; the server accessing the receiver specific information to decrypt the encrypted transfer specific encryption key; and decrypting the encrypted data using the decrypted transfer specific encryption key.

WO 2005/117331 A1

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).

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.

Published:
— *with international search report*