20000130-0
(Pat's copy)

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 99/48243**

(43) International Publication Date: 23 September 1999 (23.09.99)

(21) International Application Number: PCT/SG98/00020

(22) International Filing Date: 18 March 1998 (18.03.98)

(71) Applicant *(for all designated States except US)*: INSTITUTE OF SYSTEMS SCIENCE [SG/SG]; National University of Singapore, Heng Mui Keng Terrace, Kent Ridge, Singapore 119597 (SG).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: BAO, Feng [CN/SG]; BLK 351, Clementi Avenue 2 #04-57, Singapore 120351 (SG). DENG, Huijie [SG/SG]; 57 West Coast Lane, Singapore 127787 (SG).

(74) Agent: MCCALLUM, Graeme, David; Lloyd Wise, Tanjong Pagar, P.O. Box 636, Singapore 910816 (SG).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, 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, 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, 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 METHOD OF EXCHANGING DIGITAL DATA

(57) Abstract

A method of exchanging digital signatures (sign_A, sign_B) between a first and a second party (A, B) includes the first party (A) encrypting their signature (sign_A) and generating an authentication certificate (Cert_A), the authentication certificate (Cert_A) authenticating that the encrypted signature (C_T) is an encryption of the signature (sign_A). The first party (A) sends the encrypted signature (C_T) and the authentication certificate (Cert_A) to the second part (B). The second party (B) verifies that the encrypted signature (C_T) is an encryption of the digital signature (sign_A) of the first party (A), and if the verification is positive, the second party (B) sends its digital signature (sign_B) to the first party (A). The first party (A) verifies that the digital signature (sign_B) is the digital signature of the second party (B), and if the verification is positive the first party sends its unencrypted signature (sign_A) to the second party (B). The second party (B) verifies that the digital signature (sign_A) is the first party's digital signature, and accepts the digital signature (sign_A) if the verification is positive. If the verification is negative, the second party (B) sends the encrypted digital signature (C_T) and its digital signature (sign_B) to a third party (T). The third party (T) is independent of the first and second parties (A, B) and has a decryption key to decrypt the encrypted digital signature (C_T) of the first party (A). The third party (T) decrypts the encrypted digital signature (C_T) to obtain the first party's digital signature (sign_A), and verifies that the digital signatures (sign_A, sign_B) are the digital signatures of the first and second party (A, B) respectively. If both digital signatures (sign_A, sign_B) are verified as the digital signatures of the first and second parties (A, B), the third party (T) sends the first party's digital signature (sign_A) to the second party (B) and sends the second party's digital signature (sign_B) to the first party (A).

