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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 January 2006 (26.01.2006)

PCT

(10) International Publication Number
WO 2006/009517 A1

(51) International Patent Classification[7]: H04L 9/32

(21) International Application Number:
PCT/SG2005/000226

(22) International Filing Date: 11 July 2005 (11.07.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/590,348 23 July 2004 (23.07.2004) US

(71) Applicant *(for all designated States except US)*: **DATA SECURITY SYSTEMS SOLUTIONS PTE LTD** [SG/SG]; 371 Beach Road, #17-08/09, Keypoint, Singapore 199597 (SG).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **TAN, Teik Guan** [SG/SG]; 6 Petir Road, #09-15, Singapore 678267 (SG).

(74) Agent: **LAWRENCE Y D HO & ASSOCIATES PTE LTD**; 30 Bideford Road, #07-01 Thongsia Building, Singapore 229922 (SG).

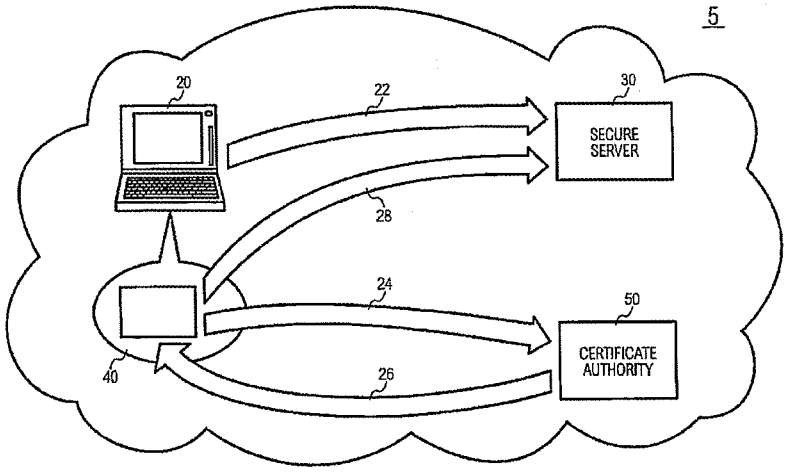
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, 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*

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.

(54) Title: SYSTEM AND METHOD FOR IMPLEMENTING DIGITAL SIGNATURE USING ONE TIME PRIVATE KEYS



(57) Abstract: The present invention relates to a system and method for implementing digital signatures using one time private keys. A system (5) implements digital signatures over a network and comprises a signing entity (20), a secure server (30), an OTPK (One Time Private Key) module (40) and an authentication server (50). The signing entity (20), the secure server (30), the OTPK module (40) and the authetication and certification server (50) are able to communicate with each other through established protocols of secure communications. The OTPK module (40) performs the function of generating only new asymmetric key pairs and also performs the functinos of generating digital signatures or digitally signing the transactions. The transactions or instructions are authorised by way of a digital signature and once the digital signature has been generated using a private key, this private key is irretrievably deleted and the deleted private key can longer be re-used).

WO 2006/009517 A1