PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06K | A2

(11) International Publication Number: WO 00/54208

(43) International Publication Date: 14 September 2000 (14.09.00)

(21) International Application Number: PCT/US00/06251

(22) International Filing Date: 10 March 2000 (10.03.00)

(30) Priority Data:
60/123,775 11 March 1999 (11.03.99) US

(71) Applicant: AMERICAN EXPRESS TRAVEL RELATED SERVICES COMPANY, INC. [US/US]; American Express Tower, World Financial Center, New York, NY 10285 (US).

(72) Inventor: PETIT, Frederic; 8880 So. Sandia Hills Drive #2180, Sandy, UT 84094 (US).

(74) Agent: SOBELMAN, Howard, I.; Snell & Wilmer L.L.P., One Arizona Center, 400 East Van Buren, Phoenix, AZ 85004-0001 (US).

(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, 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
Without international search report and to be republished upon receipt of that report.

(54) Title: METHODS AND APPARATUS FOR AUTHENTICATING THE DOWNLOAD OF INFORMATION ONTO A SMART CARD

(57) Abstract

Systems and methods for producing a digitally-computed acknowledgement of a delegated download event are disclosed. An information owner, such as the issuer of a smart card, delegates an information download to a third party. The information is downloaded from the third party to an information device, such as a smart card. The computed acknowledgement is a digital "seal" or signature (depending upon the type of cryptographic algorithm used). The seal or signature is preferably a cryptogram generated by the information device using cryptographic keys resident on the information device itself. This acknowledgement is then made available to the information owner, who may then test the cryptogram to determine whether the third party successfully completed the software download.