9705339-1

IPOS

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/30, 9/32 — A1

(11) International Publication Number: WO 96/39765

(43) International Publication Date: 12 December 1996 (12.12.96)

(21) International Application Number: PCT/US96/05317

(22) International Filing Date: 19 April 1996 (19.04.96)

(30) Priority Data:
08/462,430 5 June 1995 (05.06.95) US

(60) Parent Application or Grant
(63) Related by Continuation
US 08/462,430 (CIP)
Filed on 5 June 1995 (05.06.95)

(71) Applicant *(for all designated States except US)*: BANKERS TRUST COMPANY [US/US]; 280 Park Avenue, New York, NY 10017 (US).

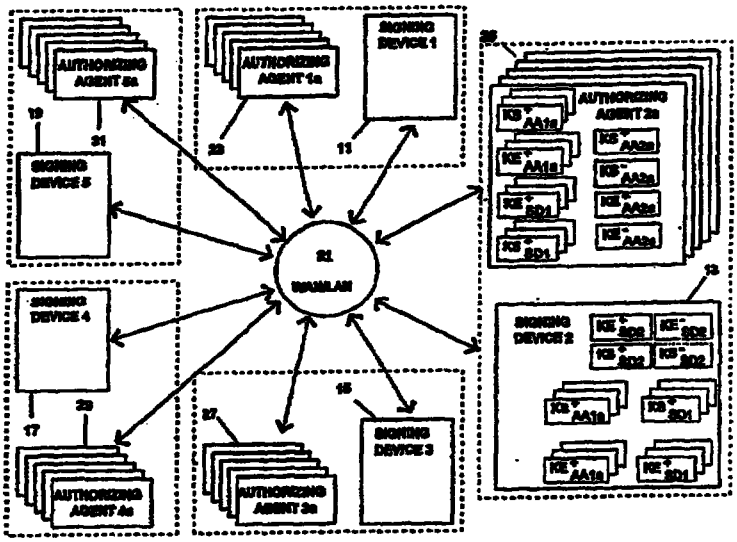
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: SUDIA, Frank, W. [US/US]; Apartment 48, 110 East 84th Street, New York, NY 10028 (US). FREUND, Peter, C. [US/US]; 8th floor, 139 East 79th Street, New York, NY 10021 (US). HUANG, Stuart, T., F. [US/US]; 2939 Van Ness Street, N.W. #907, Washington, DC 20008 (US).

(74) Agents: HUANG, Stuart, T., F. et al.; Steptoe & Johnson, L.L.P., 1330 Connecticut Avenue, N.W., Washington, DC 20036 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), 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.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: MULTI-STEP DIGITAL SIGNATURE METHOD AND SYSTEM



(57) Abstract

A multi-step signing system and method uses multiple signing devices (11, 13, 15, 17, 19) to affix a single signature which can be verified using a single public verification key. Each signing device possesses a share of the signature key and affixes a partial signature in response to authorization from a plurality of authorizing agents (23, 25, 27, 29, 31). In a serial embodiment, after a first partial signature has been affixed, a second signing device exponentiates the first partial signature. In a parallel embodiment, each signing device affixes a partial signature, and the plurality of partial signatures are multiplied together to form the final signature. Security of the system is enhanced by distributing capability to affix signatures among a plurality of signing devices and by distributing authority to affix a partial signature among a plurality of authorizing agents.