9903792-1 IPOS

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32

A1

(11) International Publication Number: WO 98/37663

(43) International Publication Date: 27 August 1998 (27.08.98)

(21) International Application Number: PCT/SE98/00206

(22) International Filing Date: 5 February 1998 (05.02.98)

(30) Priority Data:
9700587-0 19 February 1997 (19.02.97) SE

(71) Applicant *(for all designated States except US)*: POSTGIROT BANK AB (publ) [SE/SE]; S–105 06 Stockholm (SE).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: LEONARDI, Robert [SE/SE]; Gränsvägen 350, S–163 52 Spånga (SE).

(74) Agents: ÖRTENBLAD, Bertil et al.; Noréns Patentbyrå AB, P.O. Box 10198, S–100 55 Stockholm (SE).

(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, GM, GW, 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.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

1 PD
1 appl'n (pls see PF 23 Lodged on 11 NOV 1999)

1 Inv.

(54) Title: METHOD FOR AUTHORIZATION CHECK

IPC: H04L 9/32

(57) Abstract

Method for checking authorization incorporating a way to impart to a so–called smart card (SmartCard) an encryption key or equivalent key and including a way to cause a microprocessor, by means of the encryption key and at least one number, to perform a calculation whose result comprises a signature, and including a way to have said signature together with said number transferred to a system for which authorization is to be shown which includes a computer in which said encryption key is stored, said computer being programmed to carry out said calculation to obtain said signature and then to compare the latter signature with the first–mentioned signature.