

30/10/04
2004063301

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

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
13 November 2003 (13.11.2003)

PCT

(10) International Publication Number
WO 2003/094483 A3

(51) International Patent Classification⁷: **H04L 9/00**,
H04B 7/185, G06F 7/10

(21) International Application Number:
PCT/IB2003/001653

(22) International Filing Date: 29 April 2003 (29.04.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2002/1944 30 April 2002 (30.04.2002) ZA

(71) Applicant and

(72) Inventor: MEIJER, Carl, Alko [ZA/ZA]; 49 Brittany,
Tokai Villas, White Road, Tokai, 7945 Western Cape (ZA).

(74) Agent: BOWMAN GILFILLAN INC. (JOHN & KER-
NICK); P.O. Box 3511, Halfway House, Midrand 1685
(ZA).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,

CZ, DE, DK, DM, DZ, EC, 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, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD,
SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US,
UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),
Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO,
SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM,
GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— with international search report

(88) Date of publication of the international search report:
29 January 2004

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.



162162



ACTION

WO 2003/094483 A3

(54) Title: METHOD FOR PROTECTING SECRET KEY CRYPTOGRAPHIC SCHEMES

(57) Abstract: The invention discloses a method for protecting a secret key cryptographic scheme including the steps of: generating a set of strong key byte pairs for a given algorithm; selecting from the set a predetermined number of strong key byte pairs to at least partly from a secret key of predefined length; and programming an encoding device with the secret key. The invention extends to programming the secret key on a SIM card operable on a GSM network.