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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 November 2000 (30.11.2000)

PCT

(10) International Publication Number
WO 00/72506 A1

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

(21) International Application Number: PCT/GB00/01940

(22) International Filing Date: 22 May 2000 (22.05.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

09/316,805	21 May 1999 (21.05.1999)	US
09/316,804	21 May 1999 (21.05.1999)	US
09/316,686	21 May 1999 (21.05.1999)	US

(71) Applicant: INTERNATIONAL BUSINESS MACHINES CORPORATION [US/US]; New Orchard Road, Armonk, NY 10504 (US).

(71) Applicant *(for MC only)*: IBM UNITED KINGDOM LIMITED [GB/GB]; P.O. Box 41, North Harbour, Portsmouth, Hampshire PO6 3AU (GB).

(72) Inventors: HIND, John, Raithel; 5408 Harrington Grove Drive, Raleigh, NC 27613 (US). PETERS, Marcia, Lambert; 712 Lochgarton Lane, Raleigh, NC 27614 (US).

(74) Agent: LING, Christopher, John; IBM United Kingdom Limited, Intellectual Property Law Dept., Hursley Park, Winchester, Hampshire SO21 2JN (GB).

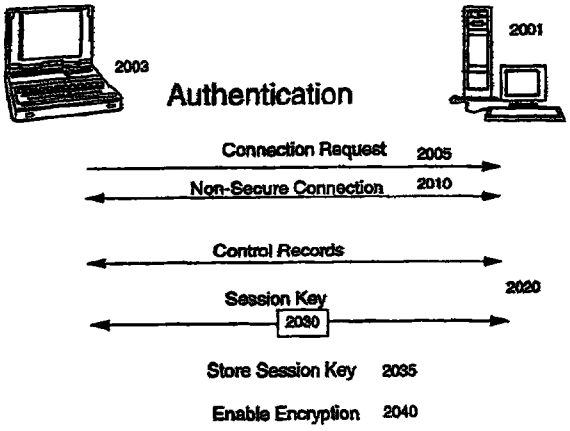
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, 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:
— *With international search report.*

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR INITIALIZING SECURE COMMUNICATIONS AMONG, AND FOR EXCLUSIVELY PAIRING WIRELESS DEVICES



(57) Abstract: A method and system for efficiently establishing secure communications between mobile devices in a radio network. The present invention utilizes public key cryptography and unique hardware identifiers to enable authorizations for access to wireless networks, such as picocells. The present invention prevents the mobile user from maintaining a plurality of secrets such as user identifier/password pairs, PINs, or encryption keys, for access to each device to which he might require access. Wireless devices distributed throughout an enterprise are enabled to be efficiently initialized for secure communications. Well-known public key cryptography and machine unique identifiers are utilised to establish a secure channel and initialize the wireless devices. Wireless devices are enabled to be paired or permanently associated by a user or a network administrator. Well known public key cryptography and machine unique identifiers are utilised to establish a secure channel and associate the devices with each other. This is extremely useful for associating a wireless headset with a telephone or associating a wireless mouse with a computer.

WO 00/72506 A1

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.