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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 August 2004 (19.08.2004)

PCT

(10) International Publication Number
WO 2004/071008 A1

(51) International Patent Classification[7]: H04L 9/32, 29/06

(21) International Application Number:
PCT/FI2004/000059

(22) International Filing Date: 6 February 2004 (06.02.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20030186 6 February 2003 (06.02.2003) FI

(71) Applicant *(for all designated States except US)*: **MERIDEA FINANCIAL SOFTWARE OY** [FI/FI]; P.o. Box 63, Helsinki FI-00381 (FI).

(72) Inventors; and

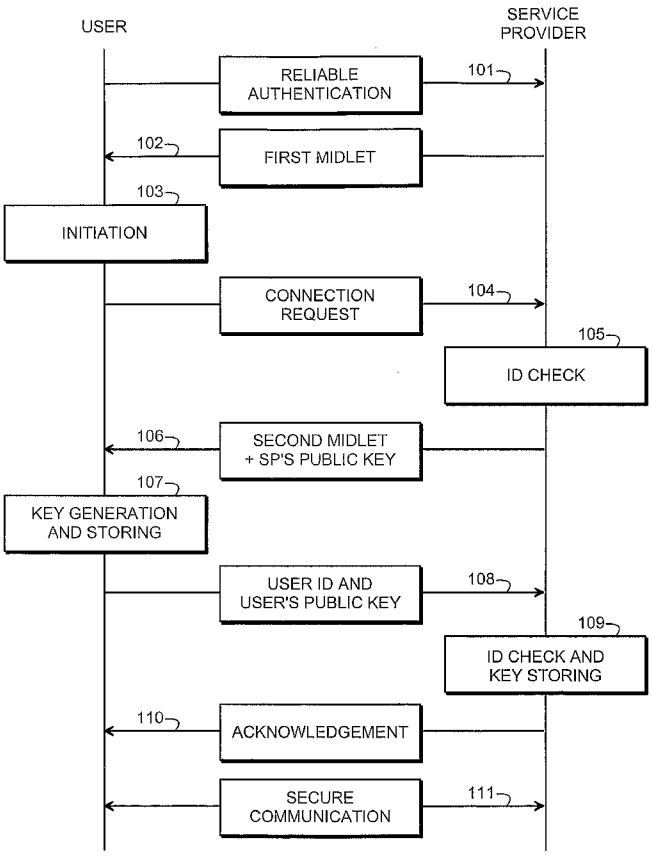
(75) Inventors/Applicants *(for US only)*: **IKONEN, Kimmo** [FI/FI]; Mäntytie 9 A 5, Helsinki FI-00270 (FI). **SUOMINEN, Markku** [FI/FI]; 4. Linja 3 B 43, Helsinki FI-00530 (FI). **LEHTI, Pekka** [FI/FI]; Pakkamestarinkatu 1b 35, Helsinki FI-00520 (FI). **LIUKKONEN, Sirpa** [FI/FI]; Vähäniityntie 12 C, Helsinki FI-00570 (FI). **OXMAN, Erno** [FI/FI]; Mistelikuja 22 B 7, Vantaa FI-01390 (FI). **WINQUIST, Niclas** [FI/FI]; Kasavuorentie 18 A 3, Kauniainen FI-02700 (FI).

(74) Agent: **BERGGREN OY AB**; P. O. Box 16, (jaakonkatu 3 A), Helsinki FI-00101 (FI).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, 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, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Continued on next page]

(54) Title: METHOD FOR SETTING UP A SECURE CONNECTION USING PUBLIC AND PRIVATE KEY GENERATED IN USER TERMINAL



(57) Abstract: A method and an arrangement are presented for setting up a secure communication connection between a user's mobile station or computer and a service provider's arrangement. The user's mobile station or computer transmits to the service provider's arrangement a connection request that contains an identification of the user placing the connection request. The service provider's arrangement responds with a response message. The user's mobile station or computer transmits to the service provider's arrangement an encryption key to be used in communication between the user's mobile station or computer and a service provider's arrangement, after which secure communication is commenced. There is also conveyed from the service provider to the user's mobile station or computer a computer program for generating cryptographic keys. The user's mobile station or computer uses it to generate cryptographic keys for use in the secure communication between the user's mobile station or computer and the service provider's arrangement.

WO 2004/071008 A1

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (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 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

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.