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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 December 2002 (19.12.2002)

PCT

(10) International Publication Number
WO 02/101980 A1

(51) International Patent Classification[7]: H04L 9/08, 9/32

(21) International Application Number: PCT/FI02/00457

(22) International Filing Date: 28 May 2002 (28.05.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20011215 8 June 2001 (08.06.2001) FI

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **NYBERG, Kaisa** [FI/FI]; Temppelikatu 3-5 A 12, FIN-00100 Helsinki (FI). **NIEMI, Valtteri** [FI/FI]; Tallberginkatu 3 as. 43, FIN-00180 Helsinki (FI).

(74) Agent: **TAMPEREEN PATENTTITOIMISTO OY**; Hermiankatu 12 B, FIN-33720 Tampere (FI).

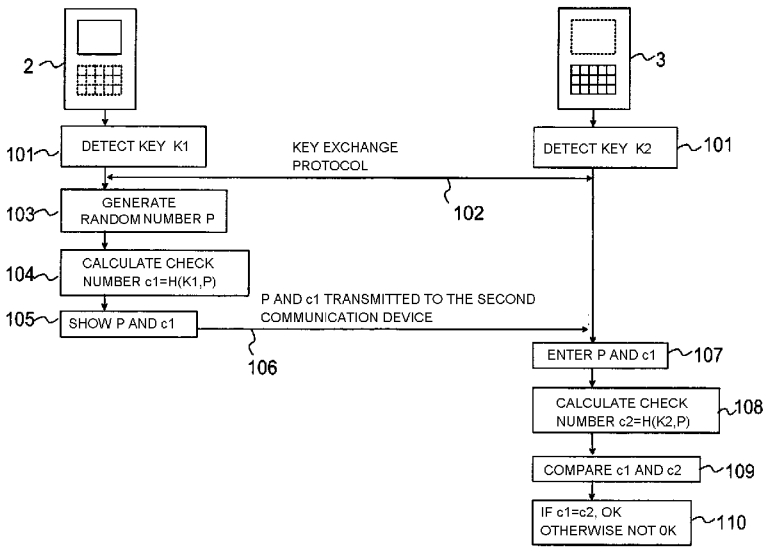
(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, 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, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK (utility model), SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, 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, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: METHOD FOR ENSURING DATA TRANSMISSION SECURITY, COMMUNICATION SYSTEM AND COMMUNICATION DEVICE



(57) Abstract: The invention relates to a method for ensuring data transmission security between a first (2) and a second communication device (3) in short-range wireless communication. To set up a secure data transmission connection, the communication devices (2, 3) conduct a key exchange stage to generate at least one shared key (K) between the communication devices. After said key exchange stage at least a first (c1) and a second check string (c2) is formed, said strings being based at least on a unique short random string and on the keys (K1, K2) generated in each communication device at said key exchange stage. Thus, the security of the connection that is set up is ensured by comparing the correspondence of said check strings (c1, c2). The invention also relates to a communication system and a communication device, in which the method will be applied.

WO 02/101980 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.