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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 October 2001 (11.10.2001)

PCT

(10) International Publication Number
WO 01/76134 A1

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

(21) International Application Number: PCT/FI01/00015

(22) International Filing Date: 8 January 2001 (08.01.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20000760 31 March 2000 (31.03.2000) FI

(71) Applicant: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

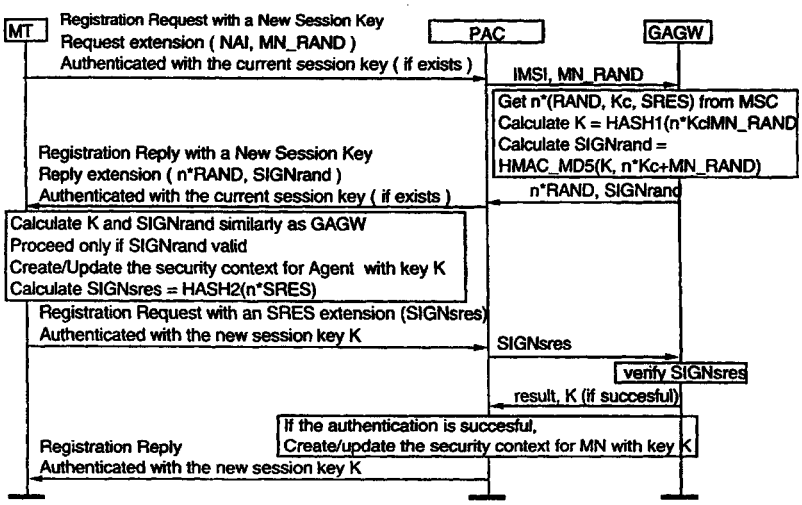
(72) Inventors: **HAVERINEN, Henry**; Arkkitehdinkatu 15 A 3, FIN-33720 Tampere (FI). **HONKANEN, Jukka-Pekka**; Aleksanterinkatu 17 A 46, FIN-33100 Tampere (FI). **KUIKKA, Antti**; Insinöörinkatu 84 C 39, FIN-33720 Tampere (FI). **ASOKAN, Nadarajah**; Ankkurinvarsi 6 K, FIN-02320 Espoo (FI). **FLYKT, Patrik**; Silmupolku 1 B 43, FIN-00380 Helsinki (FI). **ALA-LAURILA, Juha**; Mustalahdenkatu 10 A 5, FIN-33210 Tampere (FI). **RINNEMAA, Jyri**; Kaiturinkatu 16 A 5, FIN-33820 Tampere (FI). **TAKAMÄKI, Timo**; Helaraitti 1 B, FIN-33720 Tampere (FI). **VUONNALA, Raimo**; Finnoontie 54 M 33, FIN-02280 Espoo (FI). **EKBERG, Jan-Erik**; Seljatie 1 A 5, FIN-00320 Helsinki (FI). **MIKKONEN, Tommi**; Peltovainionkatu 45, FIN-33400 Tampere (FI). **AALTO, Petri**; Pärrinkuja 2, FIN-33920 Pirkkala (FI). **HONKANEN, Seppo**; Mustanhalssinkuja 11, FIN-00760 Helsinki (FI).

(74) Agent: **WALKER, Andrew**; Nokia Corporation, P.O. Box 206, FIN-00045 Nokia Group (FI).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), 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, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

[Continued on next page]

(54) Title: AUTHENTICATION IN A PACKET DATA NETWORK



(57) Abstract: Authentication method for authenticating a mobile node to a packet data network, in which a shared secret for both the mobile node and the packet data network is arranged by using a shared secret of the mobile node and a telecommunications network authentication centre. In the method, the mobile node sends its subscriber identity to the packet data network together with a replay attack protector. The packet data network obtains authentication triplets, forms a session key using them, and sends back to the mobile node challenges and a cryptographic authenticator made by using the session key. The mobile node can then form the rest of the authentication triplets using the challenges and then form the session key. With the session key, the mobile node can check the validity of the cryptographic authenticator. If the authenticator is correct, the mobile node sends a cryptographic response formed using the session key to the packet data network for authenticating itself to the packet data network.

WO 01/76134 A1

(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, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, 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.