

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
6 June 2002 (06.06.2002)

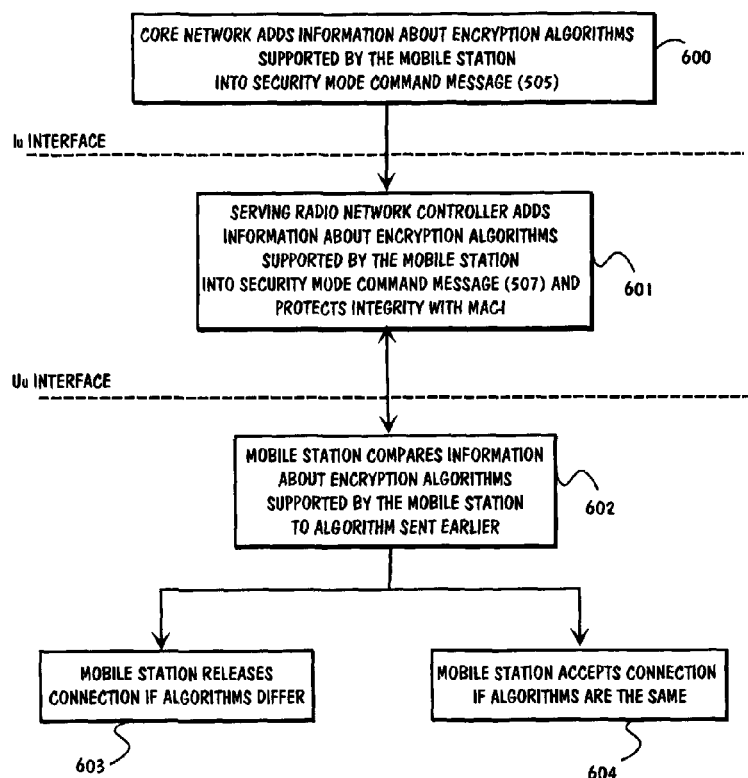
PCT

(10) International Publication Number
WO 02/45453 A1

- (51) International Patent Classification⁷: **H04Q 7/38**
- (21) International Application Number: PCT/FI01/00870
- (22) International Filing Date: 9 October 2001 (09.10.2001)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
20002613 28 November 2000 (28.11.2000) FI
20010282 14 February 2001 (14.02.2001) FI
- (71) Applicants (for all designated States except US): **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI). **NIEMI, Valtteri** [FI/FI]; Tallberginkatu 3 as. 43, FIN-00180 Helsinki (FI).
- (72) Inventor; and
(75) Inventor/Applicant (for US only): **VIALÉN, Jukka** [FI/FI]; Haltiantie 3 C, FIN-02300 Espoo (FI).
- (74) Agent: **RUUSKANEN, Juha-Pekka**; Page White & Far-
rer, 10th floor, Runeberginkatu 5, FIN-00100 Helsinki (FI).
- (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, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, 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

[Continued on next page]

(54) Title: A SYSTEM FOR ENSURING ENCRYPTED COMMUNICATION AFTER HANDOVER



SOLUTION 1

(57) Abstract: A fraudulent intruder can eavesdrop on a call by removing information about an encryption algorithm when a multimode mobile station sends an unprotected initial signaling message containing this information over the radio interface to the mobile telecommunications system. The attempt can be pre-vented in a universal mobile telecommunications system (UMTS) comprising at least two radio access networks providing mobile stations with access to at least one core network, a multimode mobile station, and at least one core network. During connection setup with a first radio access network, the multimode mobile station sends an unprotected initial signaling message that includes information about those encryption algorithms that the multimode mobile station supports when it communicates in a second radio access network. The first radio access network saves some or all the information of it. Then it composes and sends an integrity-protected message that includes information about the encryption algorithms supported by the multimode mobile station in the second radio access network.



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).

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.

Published:

- *with international search report*
- *with amended claims and statement*