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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 August 2002 (29.08.2002)

PCT

(10) International Publication Number
WO 02/067495 A3

(51) International Patent Classification[7]: H04L 9/12, 9/18, 9/32

(21) International Application Number: PCT/US02/01478

(22) International Filing Date: 18 January 2002 (18.01.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/785,722 16 February 2001 (16.02.2001) US

(71) Applicant: **MOTOROLA, INC.** [US/US]; 1303 East Algonquin Road, Schaumubrg, IL 60196 (US).

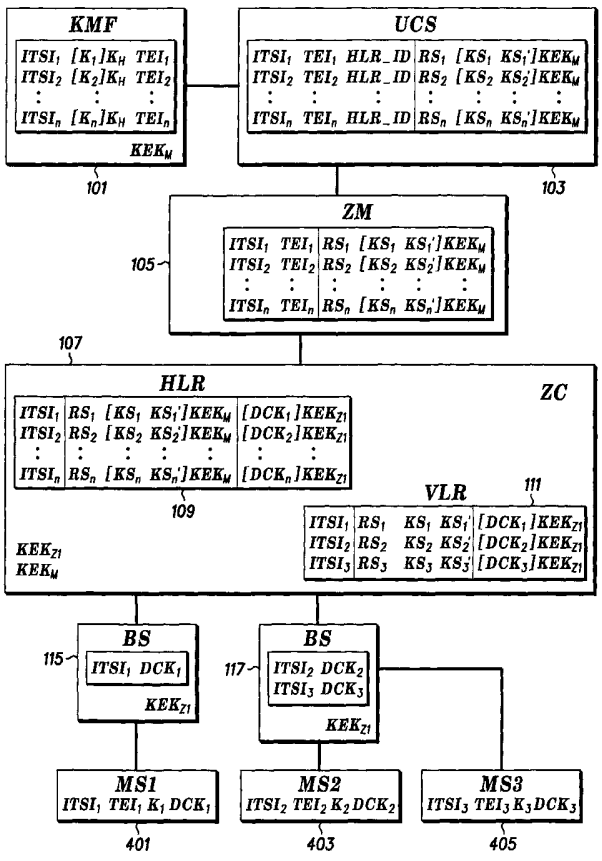
(72) Inventors: **SOWA, Hans, Christopher**; 405 Redwood Lane, Schaumburg, IL 60193 (US). **MCDONALD, Daniel, J.**; 71 Hampton Street, Cary, IL 60013 (US). **CHATER-LEA, David, J.**; 71 Heathermount Drive, Crowthorne, Berkshire RG456H (GB). **PAPPAS, Scott, J.**; 1161 Centoni Drive, Lake Zurich, IL 60047 (US). **JOHUR, Jason**; 164 Windsor Road, Maidenhead, Berkshire SL62WD (GB). **NEWKIRK, Dennis**; 470 Cranesbill Drive, West Chicago, IL 60185 (US). **KREMSKE, Randy**; 1341 Infanta Court, Woodstock, IL 60098 (US). **ANDERSON, Walter, F.**; 2111 Aspen Drive, Algonquin, IL 60102 (US).

(74) Agents: **SANTEMA, Steven, R.** et al.; MOTOROLA, INC., Intellectual Property Dept., 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

(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,

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR PROVIDING AUTHENTICATION IN A COMMUNICATION SYSTEM



(57) Abstract: A method includes receiving an authentication request from a mobile station (401) and determining whether to forward the request to an authentication agent. When it is determined to forward the request, the request is forwarded to the authentication agent (107). A random number and a random seed are received from the authentication agent (107). The random number and the random seed are forwarded to the mobile station (401). A response to the random number and the random seed from the mobile station (401) is received and forwarded to the authentication agent (107). The authentication agent (107) compares the response with an expected response. When the authentication agent (107) authenticates the mobile station (401), a derived cipher key is received from the authentication agent (107).

WO 02/067495 A3

MX, MZ, NO, NZ, PH, 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, 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*

(88) Date of publication of the international search report:
24 October 2002

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.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US02/01478

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/12, 9/18, 9/32

US CL : 380/249, 263; 713/168

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : Please See Continuation Sheet

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 6,128,389 A (CHAN et al.) 3 October 2000, (03.10.2000), column 8, lines 48-51 and 57-61; column 9, lines 1-16 and 29-53; column 10, lines 3-4 and 39-65; column 11, lines 35-67; figure 1, items 206, 106A and 206; figure 5, items 102, 204, 440, 434, 438, 506, and 514; figure 6, items 102 and 618; figure 7, steps 702, 704 , 708, 712, 714, and 718; and figure 8, steps 809, 811, and 812.	1, 3, 6 ---------- 2
A --- X	US 5,850,444 A (RUNE) 15 December 1998 (15.12.1998), column 5, lines 26-61; figure 1, item 10; figure 2, item 118; and figure 4, steps 204, 206, 208, and 210.	1, 2 ---------- 11
Y	US 5,588,062 A (ALTSCHULER et al.) 24 December 1996 (24.12.1996), column 2, lines 34-37; column 7, lines 46-48 and 65-67; column 8, lines 1-5; figure 1, item 16; figure 2, item 18; and figure 7, steps 78 and 90.	2
X	US 6,026,298 A (LAMB et al.) 15 February 2000 (15.02.2000), column 2, lines 35-40; column 5, lines 33-37 and 54-64; figure 1, items 146 and 152; and figure 5 items 636 and 658 and steps 659, 660, 665, and 666.	7-9

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 June 2002 (27.06.2002)	02 AUG 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	Authorized officer Justin T. Darrow Peggy Harrod
Facsimile No. (703)305-3230	Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/01478

C. (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,812,955 A (DENT et al.) 22 September 1998 (22.09.1998), column 17, lines 59-67; column 18, lines 1-8; column 19, lines 29-37 and 53-67; column 20, lines 1-9; figure 9, block 354; and figure 10A, steps 426a and 428a.	10, 12, 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/01478

Box I Observations where certain claims were found unsearchable (Continuation of Item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claim Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claim Nos.: 4 and 5
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
claim page 44 that contained claims 4 and 5 is missing in the application

3. ☐ Claim Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of Item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
Please See Continuation Sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.
☒ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US02/01478

BOX II. OBSERVATIONS WHERE UNITY OF INVENTION IS LACKING

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group I, claims 1-3 and 6, drawn to methods for distributing a cipher key between a mobile station and a base station.

Group II, claims 7-9, drawn to a method for forwarding encrypted session authentication information to a storage device in a non-real-time manner.

Group III, claims 10-13, drawn to systems and methods of encrypting, storing, and forwarding session authentication information.

The inventions listed as Groups I, II, and III do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: the special technical features of Group I are generating a random number and a random seed; forwarding the random number and random seed; and forwarding a cipher key if a response to the random number and random seed being authenticated; the special technical features of Group II are generating session authentication information for each of a plurality of authentication keys for use in a communication system and forwarding the encrypted session authentication information to a storage device in a non-real-time manner; the special technical feature of Group III is distributing encrypted session authentication information in a real-time manner.

Since the special technical features of any of Groups I, II, and III are not present in any of Groups II and III, I and III, and I and II, respectively, unity of invention is lacking.

Continuation of B. FIELDS SEARCHED Item 1:

IPC (7) : H04K 1/06; H04L 9/08; H04M 1/68, 1/70, 3/16; H04Q 720, 7/22, 7/28, 7/36, 7/38

US CL : 380/247, 248, 250, 258, 262, 270, 279; 713/155, 170, 176; 455/410, 411, 415, 432, 433, 435, 436, 437, 438, 439, 440

Continuation of B. FIELDS SEARCHED Item 3:

EAST(USPAT, EPO, JPO, DERWENT, USPGPUB)

search terms: random, pseudorandom, number, value, challenge, handshake, seed, initial, start, base, station, center, administrator, manager, management, compare, match, equal, authenticate, confirm, verify, validate, identify, send, forward, transmit, provide, receive, obtain, key, encrypt, encipher, encypher, scramble, directory, database, HLR, home location register, VLR, visitor location register, mobile, cellular, telephone, radio, portable, hand held, PDA, personal, palm, laptop, notebook, zone, region, cell, location, position, locality, power, activate, initialize, request