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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 April 2008 (24.04.2008)

PCT

(10) International Publication Number
WO 2008/048179 A3

(51) International Patent Classification:
H04L 9/08 (2006.01)

(21) International Application Number:
PCT/SE2007/050734

(22) International Filing Date: 11 October 2007 (11.10.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/829,954 18 October 2006 (18.10.2006) US
11/857,621 19 September 2007 (19.09.2007) US

(71) Applicant: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)** [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BLOM, Rolf** [SE/SE]; Svärdvägen 2, S-175 68 Järfälla (SE). **NÄSLUND, Mats** [SE/SE]; Stopvägen 95, S-168 36 Bromma (SE). **NORRMAN, Karl** [SE/SE]; Stigbergsgatan 32A, S-116 28 Stockholm (SE).

(74) Agent: **NORIN, Klas**; Ericsson AB, Patent Unit Service Layer and Multimedia, S-164 80 Stockholm (SE).

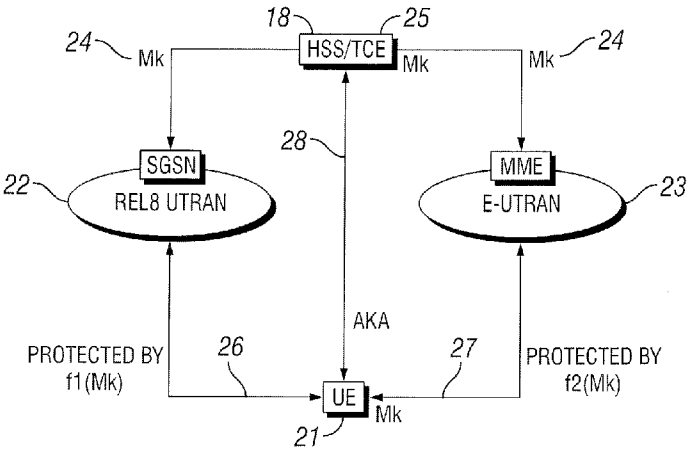
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, 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, IS, IT, LT, LU, LV, MC, MT, NL, PL, 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*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
19 June 2008

(54) Title: CRYPTOGRAPHIC KEY MANAGEMENT IN COMMUNICATION NETWORKS



(57) Abstract: An authentication server and a system and method for managing cryptographic keys across different combinations of user terminals, access networks, and core networks. A Transformation Coder Entity, TCE, (25) creates a master key, Mk, which is used to derive keys during the authentication procedure. During handover between the different access types, the Mk or a transformed Mk is passed between two authenticator nodes (42, 43, 44) that hold the key in the respective access networks when a User Equipment, UE, terminal (41, 51, 52, 53) changes access. The transformation of the Mk is performed via a one-way function, and has the effect that if the Mk is somehow compromised, it is not possible to automatically obtain access to previously used master keys. The transformation is performed based on the type of authenticator node and type of UE/identity module with which the transformed key is to be utilized. The Mk is never used directly, but is only used to derive the keys that are directly used to protect the access link.

WO 2008/048179 A3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2007/050734

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet
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)

IPC: H04L, G06F

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

SE,DK,FI,NO classes as above

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

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 20050254653 A1 (POTASHNIK, A ET AL), 17 November 2005 (17.11.2005), figure 3, paragraphs [0004],[0016]-[0019]	1-22
	--	
Y	ERICSSON: "Requirements on SAE/LTE AKA", S3-060476, 3GPPP TSG SA WG3 Security - SA3#44, 11-14 July, 2006 Tallinn, Estonia, Retrieved from: http://www.3gpp.org [2008-04-11].3.3	1-22
	--	
A	NOKIA ET AL: "Updated version of "Rationale and track of security decisions in Long Term Evolved RAN/3GPP System Architecture Evolution", 3GPP TSG SA WG3 Security-SA3#44, S3-060564, 11-14 July, 2006, Tallin, Estonia, [10.1.4]	1-22
	--	

[X] Further documents are listed in the continuation of Box C. [X] 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 but 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
24 April 2008	28 -04- 2008
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Patrik Rydman/CC Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2007/050734

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	NYBERG K : "Chryptographic algorithms for UMTS". In: European Congress on Computational Methods in Applied Sciences and Enginering 2004. Edited by Neittaanmäki et al. Jyväskylä 24-28 Juli 2004, System for distributing keys in a cell phone system, abstract -- --------	1-22

International patent classification (IPC)
H04L 9/08 (2006.01)

Download your patent documents at www.prv.se
The cited patent documents can be downloaded at www.prv.se by following the links:

- In English/Searches and advisory services/Cited documents (service in English) or
- e-tjänster/anförda dokument(service in Swedish).

Use the application number as username.
The password is **ANHYQELACG**.

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

INTERNATIONAL SEARCH REPORT
Information on patent family members

26/01/2008

International application No.
PCT/SE2007/050734

US	20050254653	A1	17/11/2005	WO	2005114897	A	01/12/2005