

Title (en)

AUTHENTICATION METHOD AND KEY GENERATING METHOD IN WIRELESS PORTABLE INTERNET SYSTEM

Title (de)

AUTHENTIFIKATIONSVERFAHREN UND SCHLÜSSELERZEUGUNGSVERFAHREN IN EINEM DRAHTLOSEN TRAGBAREN INTERNETSYSTEM

Title (fr)

PROCEDE D'AUTHENTIFICATION ET PROCEDE DE GENERATION DE CLE DANS UN SYSTEME INTERNET PORTATIF SANS FIL

Publication

EP 1864426 A4 20161123 (EN)

Application

EP 06716286 A 20060309

Priority

- KR 2006000836 W 20060309
- KR 20050019650 A 20050309
- KR 20060007226 A 20060124

Abstract (en)

[origin: WO2006096017A1] An authentication method and authorization key generation method in a wireless portable Internet system is provided. In a wireless portable Internet system, the base station and the subscriber station share an authorization key when an authentication process is performed according to a predetermined authentication method negotiated therebetween. Particularly, the subscriber station and the base station perform an additional authentication process including an authorization key-related parameter and a security-related parameter and exchanges a security algorithm and SA (Security Association) information. In addition, an authorization key is derived from one or more basic key obtained through various authentication processes as an input key of an authorization key generation algorithm. Therefore, reliability of a security-related parameter received from the receiving node can be enhanced and an authorization key having a hierarchical and secure structure can be provided.

IPC 8 full level

H04L 9/08 (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP)

H04L 9/0844 (2013.01); **H04L 9/3271** (2013.01); **H04L 2209/80** (2013.01)

Citation (search report)

- [A] US 2003226017 A1 20031204 - PALEKAR ASHWIN [US], et al
- [XI] INTEL ET AL: "Enhancing EAP/SIM and EAP/AKA Authentication with PEAP (alternative to using Temp ID for IMSI privacy)", 3GPP DRAFT; S2-023413, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG2, no. Bangkok, Thailand; 20021119, 19 November 2002 (2002-11-19), XP050241551
- [A] BERNARD ABOBA MICROSOFT DAN SIMON MICROSOFT: "PPP EAP TLS Authentication Protocol; draft-ietf-pppext-eaptls-06.txt", 5. JCT-VC MEETING; 96. MPEG MEETING; 16-3-2011 - 23-3-2011; GENEVA; (JOINT COLLABORATIVE TEAM ON VIDEO CODING OF ISO/IEC JTC1/SC29/WG11 AND ITU-T SG.16); URL: HTTP://WFTP3.ITU.INT/AV-ARCH/JCTVC-SITE/, vol. pppext, no. 6, 12 August 1999 (1999-08-12), XP015025536, ISSN: 0000-0004
- See references of WO 2006096017A1

Designated contracting state (EPC)

DE FR GB IT NL

DOCDB simple family (publication)

WO 2006096017 A1 20060914; EP 1864426 A1 20071212; EP 1864426 A4 20161123

DOCDB simple family (application)

KR 2006000836 W 20060309; EP 06716286 A 20060309