

Title (en)

METHOD AND APPARATUS FOR AUTHENTICATING SUBSCRIBER AND NETWORK IN WIRELESS INTERNET SYSTEM

Title (de)

VERFAHREN UND VORRICHTUNG ZUM AUTHENTIFIZIEREN EINES TEILNEHMERS UND NETZWERKS IN EINEM DRAHTLOSEN INTERNET-SYSTEM

Title (fr)

PROCEDE ET APPAREIL POUR AUTHENTIFIER UN ABONNE ET UN RESEAU DANS UN SYSTEME INTERNET SANS FIL

Publication

**EP 1695480 A4 20120829 (EN)**

Application

**EP 04774379 A 20040823**

Priority

- KR 2004002118 W 20040823
- KR 20030092564 A 20031217

Abstract (en)

[origin: WO2005060150A1] Provided are a method and an apparatus for authenticating a subscriber and a network, by which the subscriber and the network are provided with mutual authentication and share a key in a wireless Internet system. An authentication server generates information RES1, which is used by a mobile station for network authentication, using a private key and a first random number; and generates information XRES2, which is used for subscriber authentication, using the private key and a second random number. The mobile station generates network authentication information XRES1 using the private key and the first random number; and generates subscriber authentication information RES2 using the private key and the second random number. The mobile station compares the XRES1 with the RES1 to authenticate the network, and a gateway connected to the authentication server compares the XRES2 with the RES2 to authenticate the subscriber. Accordingly, an unauthorized user is prevented from using a network, and a subscriber's personal information is protected from being revealed to a fake server.

IPC 8 full level

**H04L 29/06** (2006.01); **H04L 9/08** (2006.01); **H04L 9/32** (2006.01); **H04L 12/56** (2006.01)

CPC (source: EP KR)

**H04L 9/0869** (2013.01 - EP); **H04L 9/14** (2013.01 - EP); **H04L 9/321** (2013.01 - EP); **H04L 9/3273** (2013.01 - EP); **H04L 63/0869** (2013.01 - EP); **H04W 12/06** (2013.01 - EP KR); **H04L 63/061** (2013.01 - EP); **H04L 63/0853** (2013.01 - EP); **H04L 2209/80** (2013.01 - EP); **H04W 12/72** (2021.01 - EP); **H04W 48/10** (2013.01 - EP); **H04W 80/04** (2013.01 - EP); **H04W 88/16** (2013.01 - EP)

Citation (search report)

- [I] WO 0203730 A1 20020110 - NOKIA CORP [FI], et al
- [I] WO 0176134 A1 20011011 - NOKIA CORP [FI]
- [A] ANDREW S. TANENBAUM: "Computer Networks (4th Edition)", 19 August 2002, PRENTICE HALL PTR, pages: 786 - 788, XP002679622
- See references of WO 2005060150A1

Designated contracting state (EPC)

FR GB

DOCDB simple family (publication)

**WO 2005060150 A1 20050630**; CN 1918843 A 20070221; CN 1918843 B 20110209; EP 1695480 A1 20060830; EP 1695480 A4 20120829; KR 100546778 B1 20060125; KR 20050060839 A 20050622

DOCDB simple family (application)

**KR 2004002118 W 20040823**; CN 200480041723 A 20040823; EP 04774379 A 20040823; KR 20030092564 A 20031217