

Title (en)

METHOD OF PROVIDING AUTHENTICATION IN A RADIOTELEPHONE NETWORK

Title (de)

VERFAHREN ZUR BEREITSTELLUNG VON AUTHENTIFIKATION IN EINEM FUNKFERNSPRECH-NETZWERK

Title (fr)

PROCEDE D AUTHENTIFICATION DANS UN RESEAU DE RADIOTELEPHONIE

Publication

EP 1668944 A2 20060614 (FR)

Application

EP 04766873 A 20041001

Priority

- EP 2004052394 W 20041001
- FR 0350638 A 20031002

Abstract (en)

[origin: WO2005032195A2] The invention relates to a method of providing authentication in a radiotelephone network. The inventive method improves security in authentication between two units in a telecommunication network, especially between a mobile terminal (MS) and the fixed network, for example between location registers (VLR, HLR) and an authentication centre (AUC), in a cellular radiotelephone network. According to the invention, prior to the generation of a signed response (SRESn), the SIM card first applies a preliminary step comprising the transformation of the random digit transmitted by the network using a transformation algorithm (AT) and, in this way, indirectly applies (E24, E27) the random digit (RAND) after the transformation thereof to the authentication algorithm (AA) in order to obtain the signed response. In addition, the SIM card stores the response produced (SRESn) for the next authentication request.

IPC 1-7

H04Q 7/38

IPC 8 full level

H04L 9/32 (2006.01); **H04W 12/06** (2009.01)

CPC (source: EP US)

H04L 9/3247 (2013.01 - EP US); **H04L 9/3271** (2013.01 - EP); **H04W 12/062** (2021.01 - EP US); **H04W 12/069** (2021.01 - EP US); **H04L 2209/80** (2013.01 - EP)

Citation (search report)

See references of WO 2005032195A2

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PL PT RO SE SI SK TR

DOCDB simple family (publication)

FR 2860672 A1 20050408; **FR 2860672 B1 20060519**; CN 1890919 A 20070103; EP 1668944 A2 20060614; WO 2005032195 A2 20050407; WO 2005032195 A3 20060420

DOCDB simple family (application)

FR 0350638 A 20031002; CN 200480035933 A 20041001; EP 04766873 A 20041001; EP 2004052394 W 20041001