Title (en)

METHOD FOR PROVIDING A SYMMETRIC KEY FOR PROTECTING A KEY MANAGEMENT PROTOCOL

Title (de)

VERFAHREN ZUM BEREITSTELLEN EINES SYMMETRISCHEN SCHLÜSSELS ZUM SICHERN EINES SCHLÜSSEL-MANAGEMENT-PROTOKOLLS

Title (fr)

PROCÉDÉ DE FABRICATION D'UNE CLÉ SYMÉTRIQUE PROTÉGEANT UN PROTOCOLE DE GESTION DE CLÉS

Publication

EP 2082521 A1 20090729 (DE)

Application

EP 07820477 A 20070924

Priority

- EP 2007060069 W 20070924
- DE 102006046017 A 20060928

Abstract (en)

[origin: WO2008037670A1] The invention relates to a method for providing a symmetric key for protecting a key management protocol, whereby cryptographic material is generated for a protocol for the encrypted transmission of media data between a subscriber device and a provider device. Said method comprises the following steps: providing a first symmetric key of the subscriber device and the provider device which is inserted in a symmetric key protection mechanism of a network protocol of a control layer to establish a communication session between the subscriber device and the provider device; providing a first time-variable parameter on the provider device end; transmitting the provided first time-variable parameter from the provider device to the subscriber device; calculating a second symmetric key for protecting the key management protocol by means of a defined function depending at least on the provided first symmetric key and the provided first time-variable parameter on the provider device end; and calculating the second symmetric key by means of the defined function depending at least on the provided first symmetric key and the transmitted first time-variable parameter on the subscriber device end.

IPC 8 full level

H04L 9/08 (2006.01)

CPC (source: EP KR US)

H04L 9/0838 (2013.01 - EP KR US); **H04L 63/0435** (2013.01 - KR); **H04L 63/0442** (2013.01 - EP US); **H04L 63/06** (2013.01 - EP KR US); H04L 2209/60 (2013.01 - EP KR US); H04L 2209/76 (2013.01 - EP KR US)

Citation (search report)

See references of WO 2008037670A1

Designated contracting state (EPC)

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

Designated extension state (EPC)

AL BA HR MK RS

DOCDB simple family (publication)

DE 102006046017 A1 20080403; **DE 102006046017 B4 20100114**; CN 101536399 A 20090916; EP 2082521 A1 20090729; JP 2010505313 A 20100218; KR 101488167 B1 20150130; KR 20090067194 A 20090624; US 2010034384 A1 20100211; US 8488795 B2 20130716; WO 2008037670 A1 20080403; WO 2008037670 B1 20080612

DOCDB simple family (application)

DE 102006046017 A 20060928; CN 200780035953 A 20070924; EP 07820477 A 20070924; EP 2007060069 W 20070924; JP 2009529672 A 20070924; KR 20097008709 A 20070924; US 31135807 A 20070924