Title (en)

DEVICE AND METHOD FOR GENERATING A SESSION KEY BETWEEN ENTITIES WITH SMALL RESOURCES

Title (de)

VORRICHTUNG UND VERFAHREN ZUR ERZEUGUNG EINES SITZUNGSSCHLÜSSELS ZWISCHEN ENTITÄTEN MIT KLEINEN RESSOURCEN

Title (fr)

DISPOSITIF ET PROCEDE POUR GENERER UNE CLE DE SESSION ENTRE DES ENTITES A FAIBLES RESSOURCES

Publication

EP 2865128 A1 20150429 (FR)

Application

EP 13730247 A 20130619

Priority

- FR 1255856 A 20120621
- EP 2013062784 W 20130619

Abstract (en)

[origin: WO2013190003A1] The present invention relates to a device and a method for establishing a session key between two entities of a communication network that may be highly heterogeneous in terms of resources. The method of the invention, based on the DiffieHellman (DH) algorithm, provides for the delegation to assistant nodes of the network of the cryptographic operations required for the calculations of the DH public value and of the DH session key for the node which is constrained in terms of resources.

IPC 8 full level

H04L 9/08 (2006.01)

CPC (source: EP US)

H04L 9/0838 (2013.01 - EP US); **H04L 9/0841** (2013.01 - US); **H04L 9/085** (2013.01 - EP US); H04L 2209/24 (2013.01 - US); H04L 2209/76 (2013.01 - EP US)

Citation (search report)

See references of WO 2013190003A1

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)

BA ME

DOCDB simple family (publication)

FR 2992509 A1 20131227; **FR 2992509 B1 20170526**; EP 2865128 A1 20150429; US 2015188700 A1 20150702; US 9843443 B2 20171212; WO 2013190003 A1 20131227

DOCDB simple family (application)

FR 1255856 A 20120621; EP 13730247 A 20130619; EP 2013062784 W 20130619; US 201314409936 A 20130619