Title (en)

METHOD FOR SECURE COMMUNICATION BETWEEN TWO DEVICES

Title (de)

VERFAHREN ZUR SICHEREN KOMMUNIKATION ZWISCHEN ZWEI GERÄTEN

Title (fr)

PROCEDE POUR UNE COMMUNICATION SECURISEE ENTRE DEUX DISPOSITIFS

Publication

EP 1391074 A1 20040225 (FR)

Application

EP 02727668 A 20020417

Priority

- FR 0201324 W 20020417
- FR 0105316 A 20010419

Abstract (en)

[origin: WO02087144A1] A method for secure communication of information between a first (25) and second module (26) whereby each module contains one of the keys of the two couples (30, 32; 31, 33) of keys, wherein a first number S and a second number A1 are randomly generated in the first module (25), a third number A2 is randomly generated in the second module (26) and wherein symmetrical verification occurs as to whether a random number (S, A1, A2) encrypted by one (25, 26) of the modules, decrypted by the other (25, 26) and retransmitted in an encrypted manner to one of said modules (25, 26) is identical to the initial random number after decryption, whereby a common session key K is autonomously created (43, 44) in each of the modules with at least three of the same numbers (S, A1, A2).

IPC 1-7

H04L 9/08; H04N 7/167

IPC 8 full level

H04L 9/08 (2006.01); **H04N 7/16** (2011.01); **H04N 7/167** (2011.01)

CPC (source: EP US)

H04L 9/0838 (2013.01 - EP US); **H04N 7/163** (2013.01 - EP US); **H04N 7/1675** (2013.01 - EP US); **H04N 21/4181** (2013.01 - EP US); **H04N 21/4367** (2013.01 - EP US)

Citation (search report)

See references of WO 02087144A1

Designated contracting state (EPC)

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

DOCDB simple family (publication)

WO 02087144 A1 20021031; CA 2444422 A1 20021031; EP 1391074 A1 20040225; FR 2823928 A1 20021025; FR 2823928 B1 20030822; US 2005033964 A1 20050210; US 7328342 B2 20080205

DOCDB simple family (application)

FR 0201324 W 20020417; CA 2444422 A 20020417; EP 02727668 A 20020417; FR 0105316 A 20010419; US 47458803 A 20031113