Title (en)

SECURE RENEWAL OF CRYPTOGRAPHIC KEYS

Title (de)

SICHERE ERNEUERUNG KRYPTOGRAPHISCHER SCHLÜSSEL

Title (fr)

RENOUVELLEMENT SÉCURISÉ DE CLEFS CRYPTOGRAPHIQUES

Publication

EP 2526646 A1 20121128 (DE)

Application

EP 10785021 A 20101119

Priority

- DE 102010001137 A 20100122
- EP 2010067833 W 20101119

Abstract (en)

[origin: WO2011088919A1] The invention relates to a method for the secure renewal of a cryptographic key k having partial keys kl and k2, which are used for secure communication between subscribers A and B, said method comprising steps of transmitting a first message from A to B, wherein the first message contains the following: MID, Na, MAC [k1] (MID, Na); transmitting a second message from B to A, wherein the second message contains the following: MID, Nb, MAC [k1] (MID, Na, Nb); wherein MID is an identification of A, Na is a number generated by A, Nb is a number generated by B and MAC [k1] (...) is the value of a one-way function MAC on the basis of the partial key kl; and determining a renewed key k' on the basis of both random numbers Na und Nb and of the partial key k2.

IPC 8 full level

H04L 9/08 (2006.01)

CPC (source: EP)

H04L 9/0891 (2013.01)

Citation (search report)

See references of WO 2011088919A1

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

DOCDB simple family (publication)

WO 2011088919 A1 20110728; DE 102010001137 A1 20110728; EP 2526646 A1 20121128

DOCDB simple family (application)

EP 2010067833 W 20101119; DE 102010001137 A 20100122; EP 10785021 A 20101119