

Title (en)

DEVICE AND METHOD FOR DIRECTING EXCHANGE FLOWS FOR PUBLIC OR NON SENSITIVE VALUES FOR CREATING COMMON SECRET KEYS BETWEEN SEVERAL AREAS

Title (de)

VORRICHTUNG UND VERFAHREN ZUR LENKUNG VON AUSTAUSCHFLÜSSEN FÜR ÖFFENTLICHE ODER NICHT VERTRAULICHE WERTE ZUR ERSTELLUNG GEMEINSAMER GEHEIMSCHLÜSSEL ZWISCHEN MEHREREN BEREICHEN

Title (fr)

DISPOSITIF ET PROCEDE POUR AIGILLER DES FLUX D'ECHANGE DE VALEURS PUBLIQUES OU NON SENSIBLES PERMETTANT DE CREER DES CLES SECRETES COMMUNES ENTRE PLUSIEURS ZONES

Publication

EP 2206276 A1 20100714 (FR)

Application

EP 08837866 A 20081010

Priority

- EP 2008063609 W 20081010
- FR 0707180 A 20071012

Abstract (en)

[origin: WO2009047325A1] The invention relates to a device and a method for directing exchange flows for public or non sensitive values for creating common secret keys between several areas in a system where entities communicate between them by trust groups, characterised in that it comprises at least the following steps: each entity generates a public value and communicates said public value to a router; said router includes a correspondence table for matching a virtual network number and the MAC addresses of the associated entities, and recovers all the public addresses transmitted by the entities by associating them with their MAC address and retransmits to each of said entities the public value of another entity belonging to the same trust group; each entity recovering the public value of another entity belonging to the same trust group then determines the value of the ciphering key common to the entities of a same trust group, and uses that key for ciphering the data to be transmitted to another entity.

IPC 8 full level

H04L 9/08 (2006.01)

CPC (source: EP US)

H04L 9/0841 (2013.01 - EP US); **H04L 63/062** (2013.01 - EP US); **H04L 63/065** (2013.01 - EP US)

Citation (search report)

See references of WO 2009047325A1

Designated contracting state (EPC)

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

Designated extension state (EPC)

AL BA MK RS

DOCDB simple family (publication)

FR 2922392 A1 20090417; **FR 2922392 B1 20110304**; EP 2206276 A1 20100714; US 2011093696 A1 20110421; WO 2009047325 A1 20090416

DOCDB simple family (application)

FR 0707180 A 20071012; EP 08837866 A 20081010; EP 2008063609 W 20081010; US 68276408 A 20081010