Title (en)
METHOD AND SYSTEM TO ENCRYPT MESSAGE USING A PROXY

Title (de)
VERFAHREN UND VORRICHTUNG ZUR VERSCHLÜSSELUNG MITTELS EINES PROXY

Title (fr)
PROCÉDÉ ET SYSTÈME DE CHIFFREMENT PAR UN PROXY.

Publication
**EP 1829277 A1 20070905 (FR)**

Application
**EP 05821572 A 20051208**

Priority
• EP 2005056613 W 20051208
• EP 04292975 A 20041210
• EP 05821572 A 20051208

Abstract (en)
[origin: EP1670172A1] The method involves encrypting a message (m) using a key (a) associated to an emitter, and sending the encrypted message in a conversion module comprising a conversion key and a conversion function. The encrypted message is converted into an encrypted message to be transmitted to the receiver by decryption by a key (b). The conversion key depends on a non trivial value raised to the power of the key (a) and of the key (b). An independent claim is also included for a system for transmitting messages between a transmitter and a receiver.

IPC 8 full level
**H04L 9/08** (2006.01); **H04L 9/30** (2006.01); **H04N 7/167** (2011.01)

CPC (source: EP KR US)
**H04K 1/00** (2013.01 - KR); **H04L 9/00** (2013.01 - KR); **H04L 9/30** (2013.01 - KR); **H04L 9/3013** (2013.01 - EP US);
**H04L 9/3066** (2013.01 - EP US); **H04N 7/1675** (2013.01 - EP US); **H04N 21/2343** (2013.01 - EP US); **H04N 21/2347** (2013.01 - EP US);
**H04N 21/4405** (2013.01 - EP US); H04L 2209/76 (2013.01 - EP US)

Citation (search report)
See references of WO 2006061420A1

Citation (examination)
• WO 03009522 A1 20030130 - FRANCE TELECOM [FR], et al
• EP 1043864 A2 20001011 - XEROX CORP [US]

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 NL PL PT RO SE SI SK TR

DOCDB simple family (publication)
**EP 1670172 A1 20060614**; AR 052652 A1 20070328; AU 2005313270 A1 20060615; AU 2005313270 B2 20100603;
BR PI0517168 A2 20090721; CA 2590008 A1 20060615; CA 2590008 C 20140401; CN 1812320 A 20060802; CN 1812320 B 20110330;
EP 1829277 A1 20070905; IL 183799 A0 20070920; IL 183799 A 20120329; JP 2008523673 A 20080703; JP 4838809 B2 20111214;
KR 101203276 B1 20121120; KR 20070100712 A 20071011; MX 2007006904 A 20070926; RU 2007121323 A 20090120;
TW 200633463 A 20060916; TW I376136 B 20121101; US 2006140397 A1 20060629; US 7724896 B2 20100525; WO 2006061420 A1 20060615;
ZA 200704815 B 20080827

DOCDB simple family (application)
**EP 04292975 A 20041210**; AR P050105182 A 20051212; AU 2005313270 A 20051208; BR PI0517168 A 20051208; CA 2590008 A 20051208;
CN 200510137325 A 20051209; EP 05821572 A 20051208; EP 2005056613 W 20051208; IL 18379907 A 20070610;
JP 2007544920 A 20051208; KR 20077013145 A 20051208; MX 2007006904 A 20051208; RU 2007121323 A 20051208;
TW 94143432 A 20051208; US 29763705 A 20051209; ZA 200704815 A 20051208