

Title (en)
METHOD FOR TRANSFERRING ENCODED MESSAGES

Title (de)
VERFAHREN ZUM TRANSFERIEREN VON VERSCHLÜSSELTEN NACHRICHTEN

Title (fr)
PROCÉDÉ DE TRANSFERT DE MESSAGES CODÉS

Publication
EP 2098039 A1 20090909 (DE)

Application
EP 07845271 A 20071130

Priority
• AT 2007000540 W 20071130
• AT 20042006 A 20061204

Abstract (en)
[origin: WO2008067575A1] Disclosed is a method for transferring encoded messages between at least two users, particularly cryptographic protocol, the message transaction taking place by inserting an authentication device which decodes the messages received from the users and sends especially encoded messages to the users. Said method comprises the following steps: a1) the user (A) sends a message (NA₁) to the authentication device (AE); a2) the authentication device (AE) creates a transaction identification record (T_{ID}); a3) the authentication device (AE) sends a message (NAE₁) containing the transaction identification record (T_{ID}) to the user (A); a4) the user (A) creates a message (NA₂) that is encoded by means of a key (SA₂) and contains the transaction identification record (T_{ID}); h) the message (NA₂) is sent to a second user (B); i) the second user (B) creates a message (NB₁) that includes the encoded message (NA₂) and is encoded by means of another key (SB); j) the message (NB₁) is sent to the authentication device (AE); k) the authentication device (AE) decodes the message (NB₁), (NA₂) with the help of the respective key (SB₁), (SA₂); l) the authentication device (AE) creates a message (NAE₂) by referring to the plain texts (A₂), (B₁) contained in the decoded messages (NA₂), (NB₁); and m) the message (NAE₂) is sent to the first user (A) and/or the second user (B).

IPC 8 full level
H04L 29/06 (2006.01); **G06F 21/31** (2013.01); **G06F 21/32** (2013.01); **H04L 12/22** (2006.01)

CPC (source: EP US)
H04L 63/0464 (2013.01 - EP US); **H04L 63/08** (2013.01 - EP US)

Citation (search report)
See references of WO 2008067575A1

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 MT NL PL PT RO SE SI SK TR

DOCDB simple family (publication)
WO 2008067575 A1 20080612; AT 504634 A1 20080615; AT 504634 B1 20081115; EP 2098039 A1 20090909; JP 2010512036 A 20100415; US 2009271616 A1 20091029; US 2012254609 A1 20121004

DOCDB simple family (application)
AT 2007000540 W 20071130; AT 20042006 A 20061204; EP 07845271 A 20071130; JP 2009538548 A 20071130; US 201213483502 A 20120530; US 45715709 A 20090602