

Title (en)
AUTHENTICATION METHOD AND DEVICE

Title (de)
AUTHENTIFIZIERUNGSVERFAHREN UND -VORRICHTUNG

Title (fr)
PROCEDE ET DISPOSITIF D'AUTHENTIFICATION

Publication
EP 1985061 A1 20081029 (FR)

Application
EP 07730922 A 20070205

Priority

- FR 2007000206 W 20070205
- FR 0601004 A 20060203
- FR 0601625 A 20060224
- FR 0601739 A 20060227

Abstract (en)
[origin: WO2007088288A1] The invention concerns an authenticating method including: a step of generating a random number (105); a step of generating a timestamping (115); a step of generating a first secret key (120); a step of truncating a message authentication code using said first secret key (125); a step of symmetrically encrypting the random number, the timestamping and the truncation (135), using a second secret key (130) to produce an authentication code (145). Preferably, during the step of generating the random number, a quantum generator (100) is used. Preferably, during the truncating step, a cryptographic message authenticator is generated using the first secret key. Preferably, during the step of symmetrically encrypting the random secret key, using the second secret key, a message digest (140) is additionally produced.

IPC 8 full level
G03H 1/00 (2006.01); **G06K 1/12** (2006.01); **G06K 9/76** (2006.01); **G06K 19/10** (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP US)
G06F 21/31 (2013.01 - EP US); **G06Q 20/3823** (2013.01 - EP US); **G06Q 20/40** (2013.01 - EP US); **G07D 7/004** (2013.01 - EP US); **G09C 1/00** (2013.01 - EP US); **H04L 9/3242** (2013.01 - EP US); **H04L 9/3297** (2013.01 - EP US); **B41M 3/14** (2013.01 - EP US); **B41M 5/24** (2013.01 - EP US); **G03H 1/0011** (2013.01 - EP US); **G06F 2221/2151** (2013.01 - EP US); **H04L 2209/20** (2013.01 - EP US); **H04L 2209/603** (2013.01 - EP US)

Citation (search report)
See references of WO 2007088288A1

Citation (examination)

- EP 2264658 A2 20101222 - YOTTAMARK INC [US]
- WO 2004081649 A2 20040923 - DIGIMARC CORP [US], et al
- DE 4410431 A1 19950928 - GIESECKE & DEVRIENT GMBH [DE]
- WO 9904364 A1 19990128 - ASSURE SYSTEMS INC [US], et al
- US 2004201873 A1 20041014 - ERICKSON RONALD R [US], et al

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)
WO 2007088288 A1 20070809; EP 1985061 A1 20081029; EP 2809030 A2 20141203; EP 2809030 A3 20150422; US 2009308530 A1 20091217; US 2012166800 A1 20120628; US 8125697 B2 20120228

DOCDB simple family (application)
FR 2007000206 W 20070205; EP 07730922 A 20070205; EP 14154203 A 20070205; US 201213405777 A 20120227; US 27821107 A 20070205