Title (en)

METHOD AND SYSTEM FOR GENERATING A LIST SIGNATURE

Title (de)

VERFAHREN UND SYSTEM ZUR ERZEUGUNG EINER LISTENUNTERSCHRIFT

Title (fr)

ABREGE DESCRIPTIF PROCEDE ET SYSTEME DE SIGNATURE DE LISTE

Publication

EP 1747639 A1 20070131 (FR)

Application

EP 05773026 A 20050518

Priority

- FR 2005001248 W 20050518
- EP 04291288 A 20040519
- EP 04291289 A 20040519
- EP 05773026 A 20050518

Abstract (en)

[origin: WO2005122466A1] The invention relates to a method for generating a list signature for a message to be signed (M), said method comprising steps which are carried out by an electronic material support (7) of a member of a list. During said step, the electronic material support only generates an electronic signature (Si) according to a sequence number (REPSEQ) supplied to the electronic material support by a certifying authority, according to evidence of belonging (SKL) to the list of members, to data (Idi, SKi) relating to the electronic material support, and optionally to a key of an authority qualified to lift the anonymity of the generated signature.

IPC 8 full level

H04L 9/32 (2006.01)

CPC (source: EP KR US)

H04L 9/32 (2013.01 - KR); **H04L 9/3255** (2013.01 - EP US); H04L 2209/42 (2013.01 - EP US); H04L 2209/463 (2013.01 - EP US); H04L 2209/56 (2013.01 - EP US)

Citation (search report)

See references of WO 2005122466A1

Citation (examination)

- "Correct System Design", vol. 2727, 1 January 2003, SPRINGER INTERNATIONAL PUBLISHING, Cham, ISBN: 978-3-642-27584-5, ISSN: 0302-9743, article SÉBASTIEN CANARD ET AL: "On Fair E-cash Systems Based on Group Signature Schemes", pages: 237 - 248, XP055274171, 032548, DOI: 10.1007/3-540-45067-X_21
- SEBASTIEN CANARD ET AL: "WCC 2003: List Signature Schemes and Application to Electronic Voting", WCC 2003, 25 March 2003 (2003-03-25), XP055274172, Retrieved from the Internet <URL:https://www.rocq.inria.fr/secret/WCC2003/program.html> [retrieved on 20160520]
- "IFIP. INTERNATIONAL FEDERATION FOR INFORMATION PROCESSING", vol. 153, 22 August 2004, ISSN: 1571-5736, article SÉBASTIEN CANARD ET AL: "Anonymous Services Using Smart Cards and Cryptography", pages: 83 - 98, XP055274173, DOI: 10.1007/1-4020-8147-2_6

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 MC NL PL PT RO SE SI SK TR

DOCDB simple family (publication)

WO 2005122466 A1 20051222; **WO 2005122466 B1 20060316**; CN 1954546 A 20070425; CN 1954546 B 20120822; EP 1747639 A1 20070131; JP 2007538443 A 20071227; JP 4818264 B2 20111116; KR 101192875 B1 20121018; KR 20070040755 A 20070417; US 2008046310 A1 20080221; US 8352380 B2 20130108

DOCDB simple family (application)

FR 2005001248 W 20050518; CN 200580015778 A 20050518; EP 05773026 A 20050518; JP 2007517338 A 20050518; KR 20067025556 A 20050518; US 59654805 A 20050518