

Title (en)

METHOD AND DEVICE FOR ANONYMOUS SIGNATURE WITH A SHARED PRIVATE KEY

Title (de)

VERFAHREN UND VORRICHTUNG ZUR ANONYMEN UNTERSCHRIFT MITTELS EINES GEMEINSAMEN PRIVATEN SCHLÜSSELS

Title (fr)

PROCEDE ET DISPOSITIF DE SIGNATURE ANONYME AU MOYEN D' UNE CLEF PRIVEE PARTAGEE

Publication

**EP 1461898 A1 20040929 (FR)**

Application

**EP 02801132 A 20021213**

Priority

- FR 0204335 W 20021213
- FR 0200107 A 20020104

Abstract (en)

[origin: WO03061193A1] The invention concerns a method and a system for anonymous cryptographic signature of a message. The method consists in completing the anonymous signature which is calculated (13) with a private key common to the set of members of a group authorized to sign and unknown to all revoked members. Said private key is updated (8, 11) at group level upon each revocation within the group and at member level only upon anonymous signature of a message by said member. The system consists of as many cards as there are members in a group and a device comprising a first calculating means.

IPC 1-7

**H04L 9/32**

IPC 8 full level

**G09C 1/00** (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP US)

**H04L 9/3255** (2013.01 - EP US)

Citation (search report)

See references of WO 03061193A1

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SI SK TR

DOCDB simple family (publication)

**WO 03061193 A1 20030724**; AU 2002364839 A1 20030730; EP 1461898 A1 20040929; FR 2834598 A1 20030711; FR 2834598 B1 20040220; JP 2005525721 A 20050825; JP 4082717 B2 20080430; US 2005169461 A1 20050804; US 7571324 B2 20090804

DOCDB simple family (application)

**FR 0204335 W 20021213**; AU 2002364839 A 20021213; EP 02801132 A 20021213; FR 0200107 A 20020104; JP 2003561157 A 20021213; US 50079205 A 20050321