Title (en)

RECOVERY OF OBSOLETE DECRYPTION KEYS

Title (de)

WIEDERHERSTELLUNG OBSOLETER ENTSCHLÜSSELUNGSSCHLÜSSEL

Title (fr)

RECOUVREMENT DE CLES DE DECHIFFREMENT PERIMEES

Publication

EP 1958371 A2 20080820 (FR)

Application

EP 06842095 A 20061205

Priority

- FR 2006051284 W 20061205
- FR 0512473 A 20051207

Abstract (en)

[origin: WO2007066039A2] The inventive method consists in recovering at least one obsolete decryption key (S<SUB>n</SUB>) for decrypting asymmetrically encrypted data items at a terminal (T) after generating a cryptographic encryption/decryption key pair stored in a cryptographic support such as a smart card (CP), in recording the obsolete decryption key, which is pre-encrypted according to a new generated encryption key, in a database (BL) accessible for a terminal user, in encrypting and decrypting said obsolete encryption key in the terminal connected to the cryptographic support according to the decryption key recorded in the cryptographic support in such a way that encrypted data items are decrypted according to the thus decrypted obsolete decryption key.

IPC 8 full level

H04L 9/08 (2006.01)

CPC (source: EP US)

H04L 9/0894 (2013.01 - EP US)

Citation (search report)

See references of WO 2007066039A2

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

Designated extension state (EPC)

AL BA HR MK RS

DOCDB simple family (publication)

FR 2894417 A1 20070608; EP 1958371 A2 20080820; US 2008292104 A1 20081127; US 8670567 B2 20140311; WO 2007066039 A2 20070614; WO 2007066039 A3 20080313

DOCDB simple family (application)

FR 0512473 A 20051207; EP 06842095 A 20061205; FR 2006051284 W 20061205; US 9642606 A 20061205