Title (en)

RECOVERY OF A MASTER KEY FROM RECORDED PUBLISHED MATERIAL

Title (de)

RÜCKGEWINNUNG EINES GRUNDSCHLÜSSELS AUS AUFGEZEICHNETER VERÖFFENTLICHUNG

Title (fr)

RECUPERATION D'UNE CLE MAITRESSE A PARTIR D'UN MATERIAU PUBLIE ENREGISTRE

Publication

EP 1145242 A2 20011017 (EN)

Application

EP 00965881 A 20000816

Priority

- EP 0008054 W 20000816
- US 38982599 A 19990903

Abstract (en)

[origin: WO0118807A2] An encryption of a master key is included with each recording of encrypted published material that requires the master key for decryption and subsequent processing. The master key is encrypted using a public key associated with a trusted authority, typically encoded on a smartcard that is associated with each authorized user. Should the smartcard be lost, or the decryption device become inoperative, one of the recordings containing the encrypted master key is sent to the trusted authority for a retrieval of the master key. The trusted authority uses the private key corresponding to the public key that was used to encrypt the master key to determine the master key. In a preferred embodiment, the trusted authority is the vendor of the smartcard or other encryption/decryption device, and provides a replacement smartcard or device containing the retrieved master key, typically for a fee, for subsequent use by the user to decrypt other recorded material in the user's collection.

IPC 1-7

G11B 20/00; G06F 1/00; H04L 9/08

IPC 8 full level

G06F 12/14 (2006.01); **G06F 1/00** (2006.01); **G06F 21/10** (2013.01); **G11B 20/00** (2006.01); **G11B 20/10** (2006.01); **H04L 9/08** (2006.01); **H04N 5/91** (2006.01); **H04N 5/913** (2006.01)

CPC (source: EP KR US)

G06F 15/00 (2013.01 - KR); **G06F 21/10** (2013.01 - EP US); **G11B 20/00086** (2013.01 - EP); **G11B 20/0021** (2013.01 - EP); **H04L 9/0897** (2013.01 - EP); **H04N 5/913** (2013.01 - EP); G06F 2211/008 (2013.01 - EP); G06F 2221/2131 (2013.01 - EP); H04L 2209/60 (2013.01 - EP); H04N 2005/91364 (2013.01 - EP)

Designated contracting state (EPC)

DE ES FR GB IT

DOCDB simple family (publication)

WO 0118807 A2 20010315; **WO 0118807 A3 20011004**; CN 1327586 A 20011219; EP 1145242 A2 20011017; EP 1145242 A3 20011205; JP 2003509881 A 20030311; KR 100748867 B1 20070813; KR 20010083940 A 20010903

DOCDB simple family (application)

EP 0008054 W 20000816; CN 00801828 A 20000816; EP 00965881 A 20000816; JP 2001522536 A 20000816; KR 20017005512 A 20010502