Title (en)

METHOD FOR CONTROLLING SECURE TRANSACTIONS USING A SINGLE PHYSICAL DEVICE, CORRESPONDING PHYSICAL DEVICE, SYSTEM AND COMPUTER PROGRAMME

Title (de)

VERFAHREN ZUR KONTROLLE SICHERER TRANSAKTIONEN ANHAND EINES EINZELNEN PHYSIKALISCHEN GERÄTS, ENTSPRECHENDES PHYSIKALISCHES GERÄT, SYSTEM UND COMPUTERPROGRAMM

Title (fr)

PROCEDE DE CONTROLE DE TRANSACTIONS SECURISEES METTANT EN OEUVRE UN DISPOSITIF PHYSIQUE UNIQUE, DISPOSITIF PHYSIQUE, SYSTEME, ET PROGRAMME D'ORDINATEUR CORRESPONDANTS

Publication

EP 1911194 A1 20080416 (FR)

Application

EP 06792517 A 20060718

Priority

- EP 2006064383 W 20060718
- FR 0507990 A 20050726

Abstract (en)

[origin: WO2007012583A1] The invention concerns a method for controlling secure transactions using a physical device (13) held by a user and bearing at least one pair of asymmetric keys, comprising a device public key (P₀) and a corresponding device private key (S₀). The invention is characterized in that said method includes the following steps: prior to implementing the physical device, a step of certifying said device public key (P₀) with a first certification key (S_T) of a particular certifying authority (10), delivering a device certificate (C₀) after verifying that said device private key (S₀) is housed in a tamper-proof zone of said physical device (13); a step of verifying said device certificate (C₀) by means of a second certification key (P_T) corresponding to the first certification key (S_T); in case of positive verification, a step of registering said user with a provider delivering a provider certificate (C_i) corresponding to the signature by said provider of said device public key (P₀) and an identifier (Id_i) of said user.

IPC 8 full level

H04L 9/32 (2006.01); **G06F 21/44** (2013.01)

CPC (source: EP US)

H04L 9/3263 (2013.01 - EP US); H04L 2209/56 (2013.01 - EP US)

Citation (search report)

See references of WO 2007012583A1

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 2007012583 A1 20070201; EP 1911194 A1 20080416; JP 2009503967 A 20090129; US 2009106548 A1 20090423

DOCDB simple family (application)

EP 2006064383 W 20060718; EP 06792517 A 20060718; JP 2008523317 A 20060718; US 99618106 A 20060718