Title (en)

METHOD AND DEVICE FOR SECURELY STORING DATA AND FOR ACCESSING SAID DATA

Title (de)

VERFAHREN UND VORRICHTUNG ZUM SICHEREN SPEICHERN VON DATEN UND ZUM ZUGREIFEN AUF DIESE DATEN

Title (fr)

PROCÉDÉ ET DISPOSITIF DE MÉMORISATION SÉCURISÉE DE DONNÉES ET D'ACCÈS À CES DONNÉES

Publication

EP 3234853 A1 20171025 (DE)

Application

EP 15813691 A 20151214

Priority

- DE 102014018889 A 20141217
- EP 2015002513 W 20151214

Abstract (en)

[origin: WO2016096117A1] The invention relates to a method for securely storing data D on a terminal by means of a portable data carrier, wherein an attribute vector A and a master key MK are stored on the portable data carrier. The method comprises the following steps: deriving a key K from a predicate P and the master key MK by means of a key derivation function KDF, wherein the predicate P is a Boolean function of the attribute vector A; encrypting the data D by means of the key K; and storing the encrypted data D together with the predicate P on the terminal. The invention further relates to a method for accessing encrypted data D by means of a portable data carrier. The method comprises the following steps: extracting the predicate P from the encrypted data and the predicate P; applying the predicate P to the attribute vector A; and, if the attribute vector A fulfills the predicate P, deriving the key K from the predicate P and the master key MK by means of the key derivation function KDF and decrypting the encrypted data D.

IPC 8 full level

G06F 21/62 (2013.01)

CPC (source: EP US)

G06F 21/6209 (2013.01 - EP US); **H04L 9/0861** (2013.01 - US); **H04L 9/0891** (2013.01 - US); **H04L 9/0897** (2013.01 - US)

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)

BA ME

DOCDB simple family (publication)

DE 102014018889 A1 20160623; EP 3234853 A1 20171025; US 2017351867 A1 20171207; WO 2016096117 A1 20160623

DOCDB simple family (application)

DE 102014018889 A 20141217; EP 15813691 A 20151214; EP 2015002513 W 20151214; US 201515536926 A 20151214