Title (en)

METHOD FOR AUTHENTICATING A PORTABLE DATA CARRIER

Title (de)

VERFAHREN ZUR AUTHENTISIERUNG EINES PORTABLEN DATENTRÄGERS

Title (fr)

PROCÉDÉ D'AUTHENTIFICATION D'UN SUPPORT DE DONNÉES PORTABLE

Publication

**EP 2893667 A1 20150715 (DE)**

Application

**EP 13747354 A 20130801**

Priority

- DE 102012017835 A 20120910
- EP 2013002319 W 20130801

Abstract (en)

[origin: WO2014037075A1] The invention relates to a method for authenticating a portable data carrier with respect to a terminal device using a public key and a private key of the original data carrier and using a public session key and a private session key of the terminal device. For said authentication, the data carrier uses a public group key as the public key and a key which is derived from a private group key associated with the public group key as the private key, said derivation being achieved using a derivation parameter. The portable data carrier uses the private group key to generate a digital signature of a data element which is required for the authentication process and into which the derivation parameter is integrated.

IPC 8 full level

**H04L 9/08** (2006.01)

CPC (source: EP US)

**H04L 9/0844** (2013.01 - EP US); **H04W 12/041** (2021.01 - EP US); **H04W 12/0471** (2021.01 - EP US); **H04W 12/069** (2021.01 - EP US); **H04W 12/108** (2021.01 - EP US); H04L 2209/80 (2013.01 - EP)

Citation (search report)

See references of WO 2014037075A1

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 102012017835 A1 20140313**; EP 2893667 A1 20150715; WO 2014037075 A1 20140313

DOCDB simple family (application)

**DE 102012017835 A 20120910**; EP 13747354 A 20130801; EP 2013002319 W 20130801