Title (en)

METHOD FOR AUTHENTICATING PAYMENT DATA, CORRESPONDING DEVICES AND PROGRAMS

Title (de)

VERFAHREN ZUR AUTHENTIFIZIERUNG VON ZAHLUNGSDATEN, ZUGEHÖRIGE VORRICHTUNGEN UND PROGRAMME

Title (fr)

PROCEDE D'AUTHENTIFICATION DE DONNEES DE PAIEMENT, DISPOSITIFS ET PROGRAMMES CORRESPONDANTS

Publication

EP 3479518 A1 20190508 (FR)

Application

EP 17733483 A 20170630

Priority

- FR 1656240 A 20160630
- EP 2017066365 W 20170630

Abstract (en)

[origin: WO2018002351A1] The invention pertains to a method for authenticating at least one datum, method implemented during a payment transaction occurring between a communication terminal of a merchant and a user device, method of the type comprising the authentication by the communication terminal of at least one message m generated by the user device, by way of a near-field wireless data link. Such a method comprises, within the user device: - a step of obtaining (10), on the basis of the message m, of a random datum t and of a hash function H, an authentication code S1; - a step of obtaining (20), on the basis of the message m, of the random datum t, of a public key Z of the communication terminal, of a first private key x of the user device and of the authentication code S1, a first signature component S2; - a step of obtaining (30), on the basis of the message m, of the random datum t, of the public key of Z of the communication terminal, of a second private key y of the user device and of the authentication code S1, a second signature component S3; - a step of transmitting (40), to the communication terminal, the authentication code S1, and the two signature components S2 and S3.

IPC 8 full level

H04L 9/32 (2006.01); **G06Q 20/34** (2012.01); **G07F 7/08** (2006.01); **H04L 9/08** (2006.01); **H04L 9/30** (2006.01)

CPC (source: EP US)

G06Q 20/3278 (2013.01 - US); **G06Q 20/352** (2013.01 - EP US); **G06Q 20/3823** (2013.01 - EP US); **G06Q 20/3825** (2013.01 - US); **G06Q 20/3829** (2013.01 - US); **G06Q 20/40975** (2013.01 - EP US); **G07F 7/0893** (2013.01 - EP US); **H04L 9/0841** (2013.01 - EP US); **H04L 9/3066** (2013.01 - EP US); **H04L 9/3218** (2013.01 - US); **H04L 9/3242** (2013.01 - US); **H04L 9/3247** (2013.01 - EP US); H04L 2209/72 (2013.01 - EP US)

Citation (search report)

See references of WO 2018002351A1

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)

WO 2018002351 A1 20180104; CA 3029154 A1 20180104; EP 3479518 A1 20190508; FR 3053549 A1 20180105; FR 3053549 B1 20180727; US 10922679 B2 20210216; US 2019228402 A1 20190725

DOCDB simple family (application)

EP 2017066365 W 20170630; CA 3029154 A 20170630; EP 17733483 A 20170630; FR 1656240 A 20160630; US 201716314174 A 20170630