Title (en)

METHOD FOR OBTAINING A BLIND SIGNATURE

Title (de)

VERFAHREN ZUM ERHALTEN EINER BLINDEN SIGNATUR

Title (fr)

PROCÉDÉ POUR OBTENIR UNE SIGNATURE AVEUGLE

Publication

EP 3899845 A1 20211027 (DE)

Application

EP 19824236 A 20191209

Priority

- DE 102018009950 A 20181218
- EP 2019025439 W 20191209

Abstract (en)

[origin: WO2020126079A1] The invention relates to a method for obtaining a blind signature for an electronic mint data record, eMD, in a subscriber, having the method steps of: generating a public key from a subscriber-generated serial number by means of the subscriber; generating an eMD by using the generated public key by means of the subscriber; blinding the generated eMD to obtain a blinded unsigned eMD by means of the subscriber; sending the blinded unsigned eMD from the subscriber to a signature publisher; obtaining a signed blinded eMD from the signature publisher by means of the subscriber; and removing the blinding to obtain a signed unblinded eMD by means of the subscriber. The invention also relates to a method for deriving a non-cash instalment from an eMD by means of a subscriber. The invention also relates to methods for checking the generated and/or obtained blind signature. Furthermore, the invention relates to a payment system for transmitting an electronic mint data record between at least two subscribers.

IPC 8 full level

G06Q 20/36 (2012.01); **G06Q 20/02** (2012.01); **G06Q 20/06** (2012.01); **G06Q 20/22** (2012.01); **G06Q 20/38** (2012.01); **H04L 9/32** (2006.01)

CPC (source: EP)

G06Q 20/02 (2013.01); **G06Q 20/0658** (2013.01); **G06Q 20/29** (2013.01); **G06Q 20/3678** (2013.01); **G06Q 20/38215** (2013.01); **G06Q 20/3823** (2013.01); **G06Q 20/3825** (2013.01); **G06Q 20/383** (2013.01); **H04L 9/0643** (2013.01); **H04L 9/3257** (2013.01); H04L 2209/56 (2013.01)

Citation (search report)

See references of WO 2020126079A1

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 102018009950 A1 20200618; EP 3899845 A1 20211027; WO 2020126079 A1 20200625

DOCDB simple family (application)

DE 102018009950 A 20181218; EP 19824236 A 20191209; EP 2019025439 W 20191209