Title (en)

METHOD FOR DERIVING A PARTIAL SIGNATURE WITH PARTIAL VERIFICATION

Title (de)

VERFAHREN ZUR ABLEITUNG EINER TEILSIGNATUR MIT PARTIELLER ÜBERPRÜFUNG

Title (fr)

PROCEDE DE DERIVATION D'UNE SIGNATURE PARTIELLE AVEC VERIFICATION PARTIELLE

Publication

EP 4158842 A1 20230405 (FR)

Application

EP 21734891 A 20210531

Priority

- FR 2005704 A 20200529
- FR 2021050983 W 20210531

Abstract (en)

[origin: WO2021240120A1] The invention relates to a method for deriving a partial signature for a subset of a set of messages, referred to as subset of messages, the method comprising: - receiving (E12-1) the set of messages and a signature of the set of messages, the signature comprising signature elements of the set of messages, - generating (E12-2) anonymised elements of the signature, - generating (E12-3) a first verification element calculated from messages other than those of the subset of messages, and - generating (E12-4) a second verification element intended to prove that the first verification element is correctly formed, and - sending to a verification entity a partial signature specific to the subset of messages, the partial signature comprising a constant number of elements comprising at least the elements of the signature of the set of anonymised messages, the first verification element and the second verification element, the partial signature being intended to be verified with only the messages of the subset of messages, characterised in that the second verification element is a function of derived values calculated from at least the other elements of the partial signature.

IPC 8 full level

H04L 9/32 (2006.01); **H04L 9/30** (2006.01)

CPC (source: EP US)

H04L 9/14 (2013.01 - US); **H04L 9/3066** (2013.01 - EP); **H04L 9/3239** (2013.01 - EP); **H04L 9/3247** (2013.01 - EP US)

Citation (search report)

See references of WO 2021240120A1

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

Designated validation state (EPC)

KH MA MD TN

DOCDB simple family (publication)

FR 3111037 A1 20211203; **FR 3111037 B1 20230526**; EP 4158842 A1 20230405; US 2023198778 A1 20230622; WO 2021240120 A1 20211202

DOCDB simple family (application)

FR 2005704 A 20200529; EP 21734891 A 20210531; FR 2021050983 W 20210531; US 202117928064 A 20210531