Title (en)

METHOD FOR DERIVING A PARTIAL SIGNATURE WITH PARTIAL VERIFICATION

Title (de)

VERFAHREN ZUM ABLEITEN EINER TEILSIGNATUR MIT PARTIELLER VERIFIKATION

Title (fr)

PROCÉDÉ DE DÉRIVATION DE SIGNATURE PARTIELLE AVEC VÉRIFICATION PARTIELLE

Publication

EP 4042633 A1 20220817 (FR)

Application

EP 20796871 A 20201006

Priority

- FR 1911300 A 20191011
- FR 2020051748 W 20201006

Abstract (en)

[origin: WO2021069827A1] The invention relates to a method for deriving a partial signature for a subset (I) of a set of messages ({m_1, …, m_n}), called subset of messages, said partial signature being intended to prove the validity of a signature of the set of messages for the messages of the subset of messages, said method, implemented by a partial signature derivation entity, comprising: - a step (E12) of receiving the set of messages ({m_1, …, m_n}) and a signature of said set of messages, said signature comprising signature elements ((q, s)) of the set of messages, - a step (E13) of deriving a first verification element (A) calculated from the messages of the set other than those of the subset of messages, and - a step (E14) of deriving a second verification element (B) intended to prove that the first verification element is formed correctly, and of sending a partial signature specific to the subset of messages to a verification entity (12), said partial signature comprising a constant number of elements comprising at least the elements of the signature of the set of messages, the first verification element (A) and the second verification element (B), said partial signature being intended to be verified with only the messages of the subset of messages.

IPC 8 full level

H04L 9/32 (2006.01)

CPC (source: EP US)

H04L 9/0861 (2013.01 - US); **H04L 9/3247** (2013.01 - EP US); **H04L 63/0421** (2013.01 - US); H04L 2209/42 (2013.01 - EP US)

Citation (search report)

See references of WO 2021069827A1

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)

FR 3102023 A1 20210416; **FR 3102023 B1 20230324**; CN 114762289 A 20220715; EP 4042633 A1 20220817; US 2023040203 A1 20230209; WO 2021069827 A1 20210415

DOCDB simple family (application)

FR 1911300 A 20191011; CN 202080083136 A 20201006; EP 20796871 A 20201006; FR 2020051748 W 20201006; US 202017768114 A 20201006