Title (en)

METHOD AND APPARATUS FOR EXCHANGING MESSAGES

Title (de)

VERFAHREN UND VORRICHTUNG ZUM AUSTAUSCHEN VON NACHRICHTEN

Title (fr)

PROCÉDÉ ET DISPOSITIF SERVANT À ÉCHANGER DES MESSAGES

Publication

EP 3603013 A1 20200205 (DE)

Application

EP 18727208 A 20180517

Priority

- EP 17175275 A 20170609
- EP 2018062916 W 20180517

Abstract (en)

[origin: WO2018224280A1] The invention relates to a method and to an apparatus for achieving cryptographic protection of a plurality of messages in a message exchange, for example, in particular the cryptographic protection being implemented by means of digital signatures and nonces. The nonces are not transmitted directly, but rather can be in particular reproducibly calculated from preceding messages, wherein a checksum of a previous message is also considered for each nonce. Said consideration is implemented in such a way that cryptographical calculations in particular intended for the creation of the digital signature and the nonce are preferably calculated one single time and, in particular, not separately for the nonce and the digital signature.

IPC 8 full level

H04L 29/06 (2006.01)

CPC (source: EP US)

H04L 9/0643 (2013.01 - US); **H04L 9/0819** (2013.01 - US); **H04L 9/3247** (2013.01 - US); **H04L 63/123** (2013.01 - EP US); **H04L 69/326** (2013.01 - US)

Citation (search report)

See references of WO 2018224280A1

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)

EP 3413530 A1 20181212; **EP 3413530 B1 20190731**; EP 3603013 A1 20200205; US 11424933 B2 20220823; US 2020169413 A1 20200528; WO 2018224280 A1 20181213

DOCDB simple family (application)

EP 17175275 A 20170609; EP 18727208 A 20180517; EP 2018062916 W 20180517; US 201816613849 A 20180517