Title (en)

SECURE METHOD FOR DATA EXCHANGE BETWEEN A TERMINAL AND A SERVER

Title (de)

SICHERES VERFAHREN ZUM DATENAUSTAUSCH ZWISCHEN EINEM ENDGERÄT UND EINEM SERVER

Title (fr)

PROCEDE SECURISE D'ECHANGE DE DONNEES ENTRE UN TERMINAL ET UN SERVEUR

Publication

EP 4062584 A1 20220928 (FR)

Application

EP 20821347 A 20201119

Priority

- FR 1913104 A 20191122
- FR 2020052130 W 20201119

Abstract (en)

[origin: WO2021099744A1] In this secure method for data exchange between a terminal (TRM) and a server (SRV): - the server uses a cryptographic module (CRY) configured to encrypt or decrypt a message based on input parameters comprising the message, a response to a challenge and a symmetric key (Ku); and - the terminal uses a white-box cryptography module (CRYBBu) constituting a white-box implementation of the cryptographic module (CRY) of the server (SRV) for this symmetric key (Ku).

IPC 8 full level

H04L 9/32 (2006.01); **G09C 1/00** (2006.01); **H04L 9/06** (2006.01)

CPC (source: EP US)

G09C 1/00 (2013.01 - EP); **H04L 9/0637** (2013.01 - EP); **H04L 9/3278** (2013.01 - EP US); **H04L 63/0435** (2013.01 - US); H04L 2209/16 (2013.01 - EP); H04L 2209/80 (2013.01 - EP)

Citation (search report)

See references of WO 2021099744A1

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 2021099744 A1 20210527; EP 4062584 A1 20220928; FR 3103591 A1 20210528; US 2023025166 A1 20230126

DOCDB simple family (application)

FR 2020052130 W 20201119; EP 20821347 A 20201119; FR 1913104 A 20191122; US 202017777906 A 20201119