

Title (en)

METHOD FOR SECURING COMMUNICATION WITHOUT MANAGEMENT OF STATES

Title (de)

VERFAHREN ZUR SICHERUNG VON KOMMUNIKATION OHNE VERWALTUNG VON ZUSTÄNDEN

Title (fr)

PROCEDE DE SECURISATION D'UNE COMMUNICATION SANS GESTION D'ETATS

Publication

EP 3625928 A1 20200325 (FR)

Application

EP 18723562 A 20180517

Priority

- FR 1754413 A 20170518
- EP 2018062974 W 20180517

Abstract (en)

[origin: WO2018211026A1] The invention relates to a method for communication between at least two communicating entities (C1, S1), a first communicating entity (C1) generating at least one data message comprising a payload (Data1) and an authentication heading (Token1), said method being characterised in that it comprises: generating a context parameter (ContextP1) comprising at least one datum representing the material configuration (CtrlProg) of the first entity (C1); generating a security profile (PRO_SEC) in the authentication heading (Token1), which defines the conditions of encoding the payload (Data1) of the message and of generating a signature (Sign1) by an algorithm (Signing_Module1) applied at least to the payload (Data1) of the message; including said signature (Sign1) in the generated message; inserting a stored identifier (C1_Id) of the first communication entity (C1) into the authentication heading (Token1); and inserting the safety profile (PRO_SEC) into the payload or into the authentication heading.

IPC 8 full level

H04L 9/32 (2006.01); **H04L 29/06** (2006.01); **H04W 12/00** (2009.01)

CPC (source: EP US)

G16Y 10/75 (2020.01 - US); **G16Y 30/10** (2020.01 - US); **H04L 9/0822** (2013.01 - US); **H04L 9/085** (2013.01 - US); **H04L 9/3234** (2013.01 - EP US); **H04L 9/3247** (2013.01 - US); **H04L 63/0435** (2013.01 - US); **H04L 63/0442** (2013.01 - US); **H04L 63/045** (2013.01 - US); **H04L 63/0876** (2013.01 - US); **H04L 63/123** (2013.01 - EP US); **H04W 12/03** (2021.01 - EP US); **H04W 12/041** (2021.01 - EP US); **H04W 12/069** (2021.01 - EP US); **H04W 12/106** (2021.01 - EP US); **H04W 12/35** (2021.01 - EP US); **H04L 63/045** (2013.01 - EP); **H04L 2209/72** (2013.01 - EP US); **H04W 4/70** (2018.02 - EP); **H04W 12/71** (2021.01 - EP US)

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 2018211026 A1 20181122; CN 111164933 A 20200515; EP 3625928 A1 20200325; FR 3066666 A1 20181123; FR 3066666 B1 20200703; US 11303453 B2 20220412; US 2021144130 A1 20210513

DOCDB simple family (application)

EP 2018062974 W 20180517; CN 201880042967 A 20180517; EP 18723562 A 20180517; FR 1754413 A 20170518; US 201816614535 A 20180517