Title (en)
METHOD FOR SECURING THE EXCHANGE OF AUTHENTICATION KEYS AND ASSOCIATED KEY MANAGEMENT MODULE

Title (de)
VERFAHREN ZUR SICHERUNG DES AUSTAUSCHS VON AUTHENTIFIZIERUNGSSCHLÜSSELN UND ZUGEHÖRIGES SCHLÜSSELVERWALTUNGSMODUL

Title (fr)
PROCÉDÉ POUR SÉCURISER UN ÉCHANGE DE CLÉS D'AUTHENTIFICATION ET UN MODULE DE GESTION DE CLÉS ASSOCIÉES

Publication
EP 3219575 A1 20170920 (EN)

Application
EP 16305296 A 20160317

Priority
EP 16305296 A 20160317

Abstract (en)
This method (100) comprises a step (130) of transmitting an authentication key to at least one communication module among a first and a second communication modules, the transmission being performed by a symmetric data encryption communication between a key server and said communication module, using a transportation key known by said communication module, The method further comprises a preliminary step (120) of transmitting the transportation key to said communication module, the preliminary transmission being performed by an asymmetric data encryption communication between the key server and said communication module using a public key generated by said communication module.

IPC 8 full level
B61L 27/00 (2006.01); **B61L 15/00** (2006.01)

CPC (source: EP)
B61L 15/0027 (2013.01); **B61L 27/70** (2022.01); B61L 2027/202 (2022.01); B61L 2205/02 (2013.01)

Citation (search report)
- [XY] DE 102011006772 A1 20121011 - SIEMENS AG [DE]
- [Y] US 2004236965 A1 20041125 - KROHN PETRI [FI]
- [Y] EP 1533971 A1 20050525 - ST MICROELECTRONICS SRL [IT]

Cited by
EP3825205A1; US2021018909A1; EP4035970A1; US11796996B2

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 3219575 A1 20170920; **EP 3219575 B1 20201104**; ES 2843697 T3 20210720

DOCDB simple family (application)
EP 16305296 A 20160317; ES 16305296 T 20160317