(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 219 575 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
20.09.2017 Bulletin 2017/38

(51) Int Cl.:
B61L 27/00 *(2006.01)* ***B61L 15/00*** *(2006.01)*

(21) Application number: **16305296.2**

(22) Date of filing: **17.03.2016**

(84) Designated Contracting States:
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 States:
BA ME
Designated Validation States:
MA MD

(71) Applicant: **ALSTOM Transport Technologies**
93400 Saint-Ouen (FR)

(72) Inventors:
- **RADOMIAK, Andre**
  3001 Heverlee (BE)
- **MAGDELYNS, Xavier**
  5380 Cortil-Wodon (BE)
- **FOSSION, Stéphanie**
  5032 Bothey (BE)
- **BAGLIVO, Stephano**
  40054 Budrio (IT)

(74) Representative: **Lavoix**
2, place d'Estienne d'Orves
75441 Paris Cedex 09 (FR)

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

(57) 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.

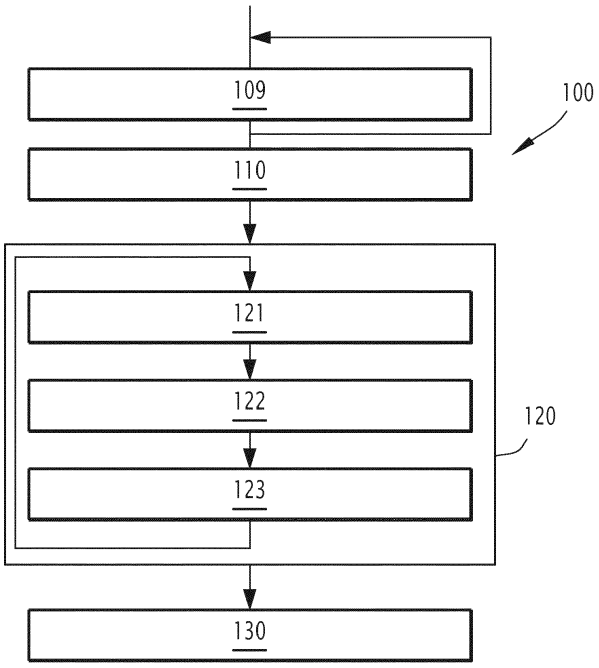

FIG.3

EP 3 219 575 A1

Description

[0001] The present invention concerns a method for securing the exchange of authentication keys used for symmetric data encryption communication between at least two communication modules.

[0002] The present invention also concerns a key management module performing this method.

[0003] At least one of said two communication modules is comprised in trackside equipment associated to a train control system and the other is an onboard communication module embedded in a railroad vehicle.

[0004] The invention is notably used for a train control system implemented according to the European Train Control System (ETCS) standard. The invention particularly relates to level 2 or 3 of the ETCS standard.

[0005] As known in the art, the ETCS standard allows the communication between trackside equipment and the railroad vehicle moving along the corresponding track. Trackside equipment is notably presented by Radio Block Centre (RBC) and Eurobalises distributed along the tracks and making it possible for example to control the speed and movement of the railroad vehicle.

[0006] In ETCS level 2 or 3, the communication between trackside equipment (e.g. RBC) and the railroad vehicle is based on a safe protocol called Euroradio protocol and constructed over the GSM-R standard and in particular, over its circuit switching or packet switching (e.g. GPRS) extension for data transmission.

[0007] To ensure a safe and secured interface between railroad communication modules, the Euroradio protocol for such type of communication makes use of symmetric authentication techniques (e.g. without data encryption).

[0008] In particular, the Euroradio protocol allows the authentication of transmitting data by symmetric authentication keys, called KMAC keys ("Key Management Authentication Code"). The authentication keys are known by each railroad communication module and shall remain secret to ensure the required safety and security level.

[0009] To maintain such safety and security level, it is known in the art that a regular updating of the authentication keys mitigates the disclosure of these KMAC keys by a malicious party. To this end, new authentication keys may be regularly transmitted by a key management module to each railroad communication module.

[0010] To keep secret the authentication keys during their distribution to their end user, namely the trackside or onboard communication module, the authentication keys are transmitted in a message encrypted using transportation keys, called also KTRANS ("Key for TRANsport").

[0011] The transportation keys are known only by the authority that issued it, the key management module, and the communication module. This last module is the recipient of the message containing the authentication keys.

[0012] However, such method for securing the distribution of transportation keys (KTRANS for ETCS) is not completely satisfying.

[0013] Particularly, the confidentiality of initialization (i.e. first distribution of the transportation key into the communication modules) and its update are based on a human procedure, hence opening potential weakness on the transportation key disclosure. Moreover, a secured human procedure requires a heavy and constraining procedure that jeopardizes the regular update of the transportation key, leading to a degradation of the security level with time.

[0014] One aim of the invention is to provide a method for securing the exchange of authentication keys having a security level which does not degrade with time.

[0015] To this end, the invention concerns a method for securing the distribution of authentication keys used for symmetric data authenticated communication between at least two communication modules, at least a first and a second communication modules, the first communication module being comprised in trackside equipment associated to a train control system and the second communication module being onboard a railroad vehicle travelling on a track managed by said train control system, the method comprising a step of transmitting an authentication key to at least one communication module among the first and 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 being characterized in that it further comprises a preliminary step 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.

[0016] The method according to the invention may comprise one or more of the following feature(s), taken in isolation, or according to any one of any technically feasible combination:

- the preliminary step of transmitting the transportation key comprises the following sub-steps receiving from said communication module, a certificate including a public key; encrypting the transportation key into an encrypted message using said public key, and transmitting the encrypted message including the transportation key to said communication module, the encrypted message being decrypted by said communication module using a session key derived from said public key;
- the preliminary step of transmitting the transportation key is performed using a Transport Layer Security protocol;
- the preliminary step of transmitting the transportation key comprises a remote authentication of the certif-

icate;

- the train control system is implemented according to an European Train Control System standard;
- the communication between any communication modules is a wireless or wired communication according to an Euroradio protocol; and
- further comprising a step of delivering to each communication module a certificate including a public key for the asymmetric data encryption communication, said step being implemented before the preliminary step of transmitting the transportation key;

[0017] The present invention concerns also a key management module for securing the distribution of authentication keys used for symmetric data authenticated communication between at least two communication modules, at least a first and a second communication modules, the first communication module being comprised in trackside equipment associated to a train control system and the second communication module being onboard a railroad vehicle travelling on a track managed by said train control system.

[0018] The key management module is able to transmit an authentication key to at least one communication module among the first and 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.

[0019] The key management module is characterized in that it is further able to transmit the transportation key to said communication module, the 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.

[0020] The invention will be better understood, upon reading of the following description, taken solely as an example, and made in reference to the following drawings, in which:

- figure 1 is a schematic view of a railroad vehicle traveling on a railroad track and managed by a train control system, the train control system comprising a key management module according to the invention;
- figure 2 is a schematic view of the key management module of figure 1; and
- figure 3 is a general flow chart of steps of the method according to the invention.

[0021] A railroad vehicle 10 travelling on a railroad track 12 is illustrated on figure 1.

[0022] The vehicle 10 is for example a passenger train.

[0023] In general case, the term "railroad vehicle" refers to any guided vehicle, i.e. any vehicle capable of travelling on a railroad track.

[0024] The vehicle 10 comprises notably a plurality of onboard systems 13, allowing the control of the vehicle 10, and an onboard communication module 14, able to provide a wireless communication between the onboard systems 13 and exterior systems, such as a control system 18, as it will be explained below.

[0025] The movement of the vehicle 10 on the railroad track 12 is managed by a train control system 18.

[0026] The train control system 18 is implemented preferably according to the European Train Control System standard, which is usually denoted as ETCS standard, more preferably in its level 2 or 3.

[0027] The train control system 18 comprises a control center 20, located away from the railroad track 12, and trackside equipment 22 distributed along the railroad track 12 or concentrated and connected to the control center 20 by a suitable network 24.

[0028] Trackside equipment 22 comprises notably a plurality of trackside entities, 26A to 26N. Each trackside entity 26A to 26N is associated to a section of the railroad track 12 and able to collect and transmit to the control center 20 at least some data relative to the vehicle 10 when it is moving on the associated section.

[0029] Each trackside entity 26A to 26N is further able to communicate with the railroad vehicle 10 over a wireless bi-directional link, in order to exchange data related for example to the authorized speed of movement on the associated section, movement permissions on this section, etc., in one direction, and the position of the vehicle, etc., in the other direction.

[0030] In particular, each trackside entity 26A to 26N comprises a railroad communication module 28A to 28N performing the data exchange with the control center 20 and with the onboard communication module 14 of the vehicle 10.

[0031] The wireless communication between the communication modules 28A to 28N and 14 is constructed over the GSM-R standard and in particular, over its circuit switching or packet switching (e.g. GPRS) extension for data transmission.

[0032] Data transmission between modules 28A to 28N and 14 is a data transmission using a symmetric data authentication technique.

[0033] This data transmission responds to a required safety level, defined by railroad authorities.

[0034] When the train control system 18 is implemented according to the ETCS standard, the authentication data transmission between the modules 28A to 28N and 14 or between 28A to 28N over the network 24 is implemented according to the Euroradio protocol known in the art and used in the ETCS standard.

[0035] The railroad communication modules 28A to 28N are implemented in a similar way. Thus, only the railroad communication module 28A will be explained in details below.

[0036] The control center 20 manages the trackside equipment 22 in function of the data collected by the trackside entities 26A to 26N.

[0037] The control center 20 comprises a key manage-

ment module 34 distributing the symmetric keys to the railroad communication modules 28A to 28N and the onboard communication module 14.

[0038] The key management module 34 and the communication modules 28A and 14 are illustrated more in details on figure 2.

[0039] In reference to figure 2, the key management module 34 comprises a first transceiver 41 for a direct wireless communication with the onboard communication module 14 of the vehicle 10, a second transceiver 42 for the communication with the railroad communication module 28A of the trackside entity 26A via the network 24, and a key server 43, providing symmetric keys for wireless communication link between the railroad communication modules 28A to 28N and the onboard communication module 14 or wired communication between 28A to 28N.

[0040] In one embodiment of the invention, the key management module 34 is connected to a certification authority module 44, also called remote controller, able to deliver and to verify certificates at the purpose of the communication modules 28A,14 and key management module 34. The remote controller is, for example, able to deliver a certificate including a public key for the asymmetric cryptographic technique to each key manager 48,51.

[0041] The railroad communication module 28A comprises a first transceiver 46 for wireless communication with the onboard communication module 14, a second transceiver 47 for communication with the key management module 34, via network 24, and a key manager 48 allowing the encrypted and/or authenticated data transmission for wireless communication between the railroad communication modules 28A to 28N and the onboard communication module 14 or wired communication between modules 28A to 28N over network 24. The transceiver 47 communicates also with the certification authority module 44 for the reception or verification of certificates at the purpose of the key manager 48

[0042] The onboard communication module 14 of the vehicle 10 comprises a transceiver 50 for wireless communication both with the railroad communication module 28A of the trackside entity 26A and the key management module 34 of the control center 20 and the certification authority module 44, and a key manager 51 allowing the encrypted or authenticated data transmission for wireless communication between the railroad communication modules 28A to 28N and the onboard communication module 14 or the certification authority module 44 directly, when this module 44 has an embedded communication module, or via the key management module 34 otherwise.

[0043] To perform a symmetric data authentication technique for the exchange of data between one railroad communication modules 28A to 28N and the onboard communication module 14, or between modules 28A to 28N, each key manager 48, 51 of each communication module 28A, 14 comprises a same plurality of authentication keys used to encrypt or authenticate data transmitted between these modules.

[0044] Thus, for example, data transmitted from the onboard communication module 14 to the railroad communication module 28A is encrypted or authenticated by the transceiver 50 using one or several authentication keys stored in both key managers 48, 51.

[0045] When the first transceiver 46 of the railroad communication module 28A receives this data, it authenticates the data using the same authentication keys.

[0046] When the train control system 18 is implemented according to the ETCS standard, the authentication keys are called KMAC keys ("Key Management Authentication Code").

[0047] The authentication keys are generated by the key server 43 of the key management module 34.

[0048] The authentication keys are then distributed by the key server 43 to each communication module 28A, 14 according to a method 100 for securing the exchange of authentication keys according to the invention.

[0049] Each key manager 48, 51 is further able to generate a public key and an associated private key for implement an asymmetric cryptographic technique as it will be explained by the method 100.

[0050] The method 100 will be described hereinafter in reference to figure 3 presenting a general flow chart of its steps.

[0051] Initially, the authentication keys are generated by the key server 43.

[0052] During the step 109, the remote controller 44 delivers a certificate including a public key for the asymmetric cryptographic technique to each key manager 48, 51.

[0053] Then, the step 109 is repeated for each railroad communication module 28A of the trackside entity 26A.

[0054] Then, during step 110, the key server 43 generates one or several transportation keys. A transportation key is generated for each communication module 28A, 14.

[0055] The transportation keys are used to encrypt or decrypt messages containing the authentication keys exchanged between the control center 20 and the corresponding communication module, using a symmetric cryptographic technique as it will be explained below.

[0056] It shall be noted that the transportation keys may be different for different communication modules 28A and 14, but they are all known by the key server 43.

[0057] During the next step 120, the key server 43 transmits the generated transportation keys to the corresponding communication modules 28A, 14 via the first or the second transceiver 41, 42 using an asymmetric data cryptographic technique.

[0058] In particular, this step 120 includes several substeps.

[0059] During the first sub-step 121, the first transceiver 41 of the key management module 34 initializes a securing connection with the onboard communication module 14 according for example to the TLS (Transport Layer

Security) protocol. The TLS protocol is defined for example in the RFC 6176 document.

[0060] In particular, during this sub-step 121, the first transceiver 41 and the transceiver 50 initialize a connection using a handshaking technique.

[0061] Then, the first transceiver 41 exchanges certificates from the transceiver 50 of the onboard communication module 14. The certificates include in particular a public key generated by the key manager 51 of the onboard communication module 14.

[0062] In one embodiment of the invention, the remote controller 44 verifies the certificate and if its authentication is not successful, reinitializes the connection with the transceiver 50.

[0063] During the next sub-step 122, the first transceiver 41 encrypts the transportation keys generated for the onboard communication module 14 using a session key derived from the public key of the received certificate.

[0064] During the next sub-step 123, the first transceiver 41 transmits the encrypted message to the transceiver 50 of the onboard communication module 14. The transceiver 50 decrypts this message using the session key established in sub-step 122.

[0065] Then, the steps 121 to 123 are repeated in a similar way in order to transmit the corresponding transportation keys to the railroad communication module 28A of the trackside entity 26A. In this case, the sub-steps 121 to 123 are performed by the second transceiver 42 of the key management module 34.

[0066] During the next step 130, for the transmission of new authentication keys to a recipient communication module, the first or the second transceiver, 41 or 42, generates a message containing the new authentication keys, the message contained authentication keys being encrypted according to a symmetric cryptographic technique similar to the symmetric cryptographic technique used for the communication between the railroad communication modules 28A and the onboard communication module 14. This encryption is performed using the transportation keys specific of the recipient communication module.

[0067] Then, the first or the second transceivers 41, 42 transmits this message to the recipient communication modules 28A and 14, which decrypts it using the transportation keys. The extracted new authentication key is stored into the key managers 48 or 51.

[0068] An authentication key is thus stored in both key managers 48 and 51 and can be further used for the encrypted data transmission between the communication modules 28A and 14 or between 28A and 28N.

[0069] The method 100 is repeated each time a transportation key update is necessary. This allows maintaining the required security level of the encrypted data transmission with time.

[0070] The method according to the invention provides a transportation keys initialization and update in a particularly simple way. The initialization and update can be done remotely and does not need a local intervention on the remote equipment, trackside or trainborne.

[0071] The invention further ensures the required safety and security level of the train control system and is particularly useful to mitigate the risk of transportation keys disclosure.

Claims

1. Method (100) for securing the distribution of authentication keys used for symmetric data authenticated communication between at least two communication modules (14, 28A, ..., 28N), at least a first and a second communication modules (14, 28A, ..., 28N), the first communication module (28A, ..., 28N) being comprised in trackside equipment (22) associated to a train control system (18) and the second communication module (14) being onboard a railroad vehicle (10) travelling on a track (12) managed by said train control system (18),
the method (100) comprising a step (130) of transmitting an authentication key to at least one communication module (14, 28A, ..., 28N) among the first and second communication modules, the transmission being performed by a symmetric data encryption communication between a key server (43) and said communication module (14, 28A, ..., 28N), using a transportation key known by said communication module (14, 28A, ..., 28N),
the method (100) being **characterized in that** it further comprises a preliminary step (120) of transmitting the transportation key to said communication module (14, 28A, ..., 28N), the preliminary transmission being performed by an asymmetric data encryption communication between the key server (43) and said communication module (14, 28A, ..., 28N) using a public key generated by said communication module (14, 28A, ..., 28N).

2. Method (100) according to claim 1, wherein the preliminary step (120) of transmitting the transportation key comprises the following sub-steps:

   - receiving (121) from said communication module (14, 28A, ..., 28N), a certificate including a public key;
   - encrypting (122) the transportation key into an encrypted message using said public key;
   - transmitting (123) the encrypted message including the transportation key to said communication module (14, 28A, ..., 28N), the encrypted message being decrypted by said communication module (14, 28A, ..., 28N) using a session key derived from said public key.

3. Method (100) according to claim 1 or 2, wherein the preliminary step (120) of transmitting the transportation key is performed using a Transport Layer Se-

curity (TLS) protocol.

4. Method (100) according to claim 3, wherein the preliminary step (120) of transmitting the transportation key comprises a remote authentication of the certificate.

5. Method (100) according to anyone of the preceding claims, wherein the train control system (18) is implemented according to an European Train Control System standard.

6. Method (100) according to claim 5, wherein the communication between any communication modules (14, 28A, ..., 28N) is a wireless or wired communication according to an Euroradio protocol.

7. Method (100) according to anyone of the preceding claims, further comprising a step (109) of delivering to each communication module (14, 28A, ..., 28N) a certificate including a public key for the asymmetric data encryption communication, said step being implemented before the preliminary step (120) of transmitting the transportation key.

8. Key management module (34) for securing the distribution of authentication keys used for symmetric data authenticated communication between at least two communication modules (14, 28A, ..., 28N), at least a first and a second communication modules (14, 28A, ..., 28N), the first communication module (28A, ..., 28N) being comprised in trackside equipment (22) associated to a train control system (18) and the second communication module (14) being onboard a railroad vehicle (10) travelling on a track (12) managed by said train control system (18),
the key management module (34) being able to transmit an authentication key to at least one communication module (14, 28A, ..., 28N) among the first and second communication modules, the transmission being performed by a symmetric data encryption communication between a key server (43) and said communication module (14, 28A, ..., 28N), using a transportation key known by said communication module (14, 28A, ..., 28N),
the key management module (34) being **characterized in that** it is further able to transmit the transportation key to said communication module (14, 28A, ..., 28N), the transmission being performed by an asymmetric data encryption communication between the key server (43) and said communication module (14, 28A, ..., 28N) using a public key generated by said communication module (14, 28A, ..., 28N).

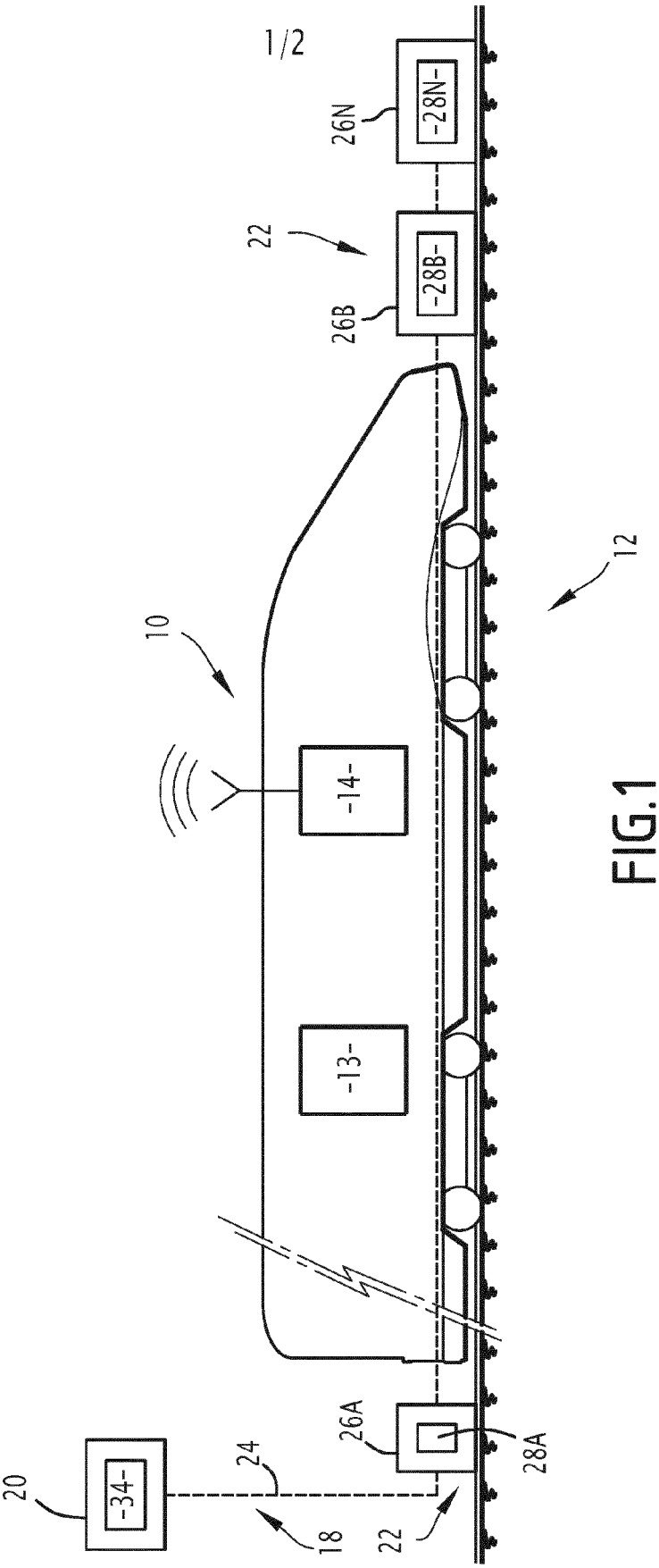

FIG.1

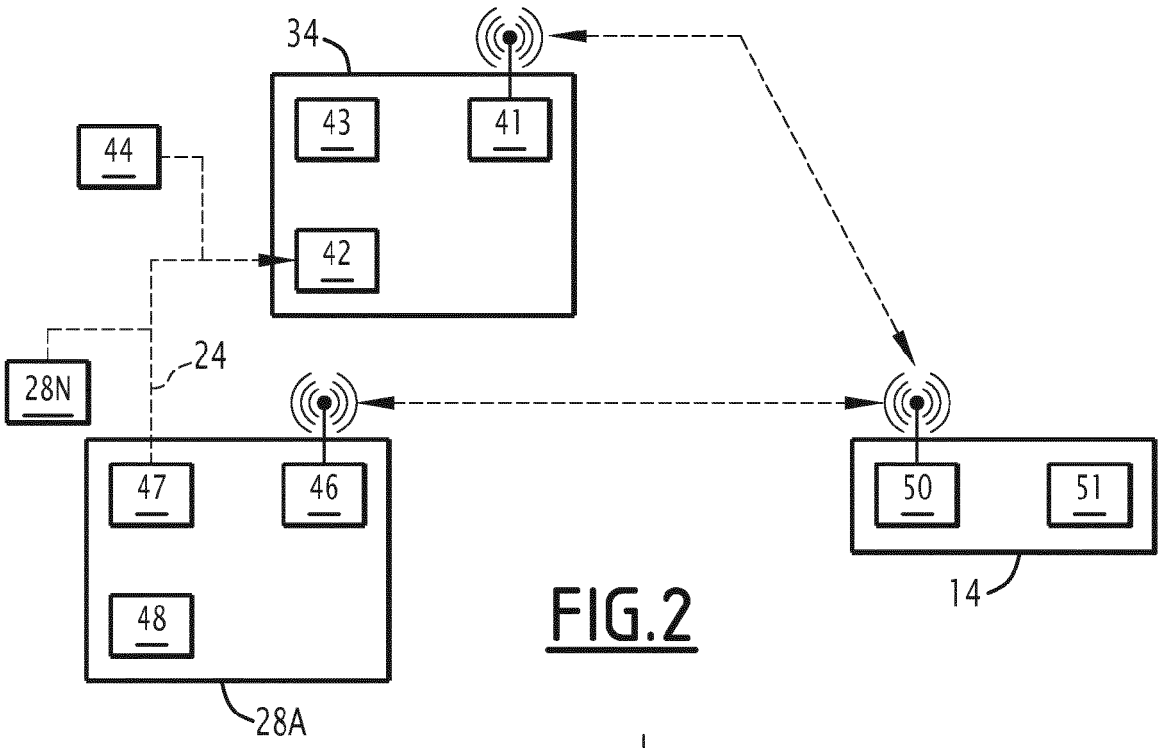
34
43
41
44
42
24
28N
47
46
48
28A
50
51
14

FIG.2

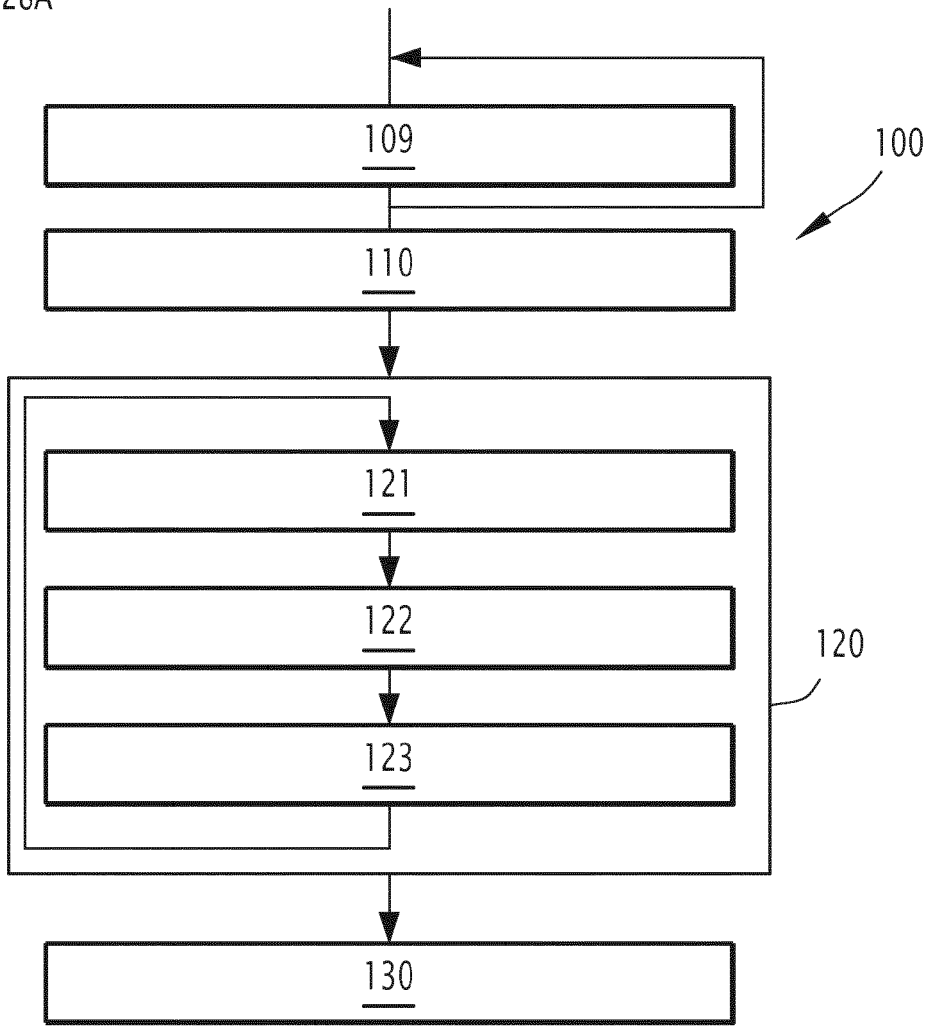
109
110
100
121
122
123
120
130

FIG.3

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 16 30 5296

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X Y	DE 10 2011 006772 A1 (SIEMENS AG [DE]) 11 October 2012 (2012-10-11) * paragraphs [0004] - [0049]; figures 1-6 * -----	1,3,5,6,8 2,4,7	INV. B61L27/00 B61L15/00
Y	US 2004/236965 A1 (KROHN PETRI [FI]) 25 November 2004 (2004-11-25) * paragraphs [0065], [0097] - [0166]; figures 1-8 * -----	2,4,7	
Y	EP 1 533 971 A1 (ST MICROELECTRONICS SRL [IT]) 25 May 2005 (2005-05-25) * paragraphs [0006] - [0007] * -----	2	

TECHNICAL FIELDS SEARCHED (IPC)

B61L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	2 September 2016	Mäki-Mantila, M

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 16 30 5296

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

02-09-2016

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 102011006772 A1	11-10-2012	CN 103459234 A	18-12-2013
		DE 102011006772 A1	11-10-2012
		EP 2658764 A1	06-11-2013
		WO 2012136525 A1	11-10-2012
US 2004236965 A1	25-11-2004	NONE	
EP 1533971 A1	25-05-2005	EP 1533971 A1	25-05-2005
		US 2005125670 A1	09-06-2005

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82