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

(11) **EP 4 116 944 A1**

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
11.01.2023 Bulletin 2023/02

(21) Application number: **22182196.0**

(22) Date of filing: **30.06.2022**

(51) International Patent Classification (IPC):
G07C 5/08 *(2006.01)*

(52) Cooperative Patent Classification (CPC):
G07C 5/085; G07C 7/00

(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:
KH MA MD TN

(30) Priority: **05.07.2021 SE 2150872**

(71) Applicant: **Scania CV AB**
151 87 Södertälje (SE)

(72) Inventors:
- **LOHAGE, Arne**
  167 38 Bromma (SE)
- **GRUNDSTRÖM, Tobias**
  647 31 Mariefred (SE)

(74) Representative: **Scania CV AB**
Patents, GP 117kv
151 87 Södertälje (SE)

(54) CONTROL UNIT AND METHOD FOR REMOTELY CONTROLLING A TACHOGRAPH

(57) The present disclosure relates to techniques in the context of vehicles, and more specifically to methods, for use in a tachograph and in a control unit arranged in a vehicle, for remotely controlling the tachograph from the control unit. According to a first aspect a method comprises communicating S21, S23 pairing request and a pairing accept between the tachograph 20 and the control unit 10 to enter a paired state. The method further comprises receiving S25 a message identifying a driver card inserted in the tachograph, obtaining S26 authentication data of a driver present in the vehicle, and authenticating S28 the driver present in the vehicle by comparing the obtained authentication data with driver identity data of the inserted driver card obtained from a driver database. The method further comprises entering S210 a remote-control state in which the control unit is enabled to remotely control the tachograph via the secure connection, in response to the authenticating S28 being successful. The disclosure also relates to a control unit or tachograph configured to perform the corresponding methods, to a vehicle comprising the control unit, to a computer program and to a computer-readable medium.

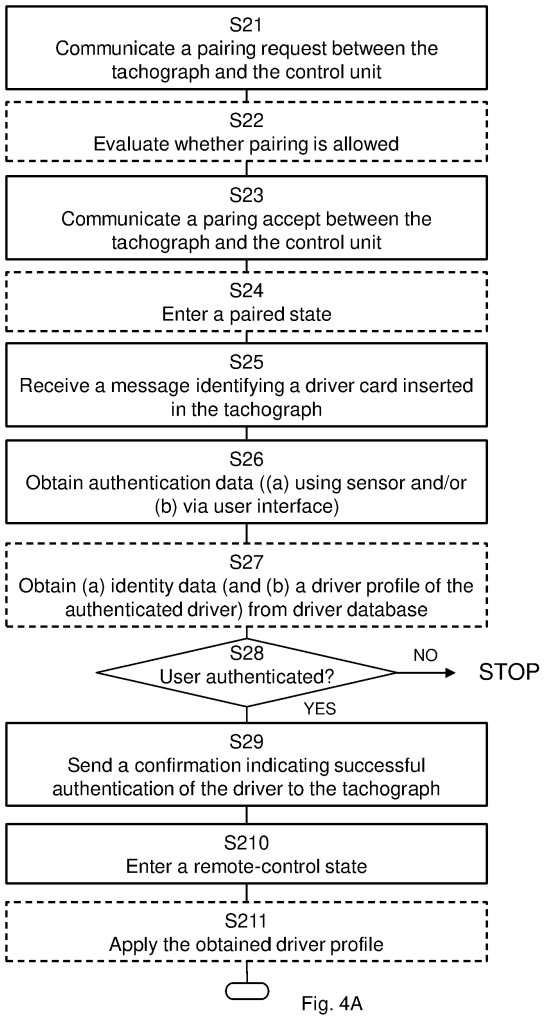

Fig. 4A

EP 4 116 944 A1

Description

Technical field

[0001] The present disclosure relates to techniques in the context of vehicles, and more specifically to methods, for use in a tachograph and in a control unit arranged in a vehicle, for remotely controlling the tachograph from the control unit. The disclosure also relates to a control unit or tachograph configured to perform the corresponding methods, to a vehicle comprising the control unit, to a computer program and to a computer-readable medium.

Background

[0002] Tachographs record information about driving time, speed and distance. Tachographs are used to make sure drivers and employers follow the rules on drivers' hours. Hence, the tachograph is a legal control unit in the sense that it is mandatory for vehicles to be equipped with such a unit (when not excluded from driver hours legislation). The driver is obliged to enter data into the tachograph, and it is currently done using buttons on the actual tachograph and viewing the display of the tachograph itself. It is well known that the user interface is not very user friendly and that many mistakes are made by the drivers when entering data into the tachograph.

[0003] Proposals have been given during many years regarding how to improve the driver interface of the tachograph, but it has rarely been implemented for security reasons. A main problem has been that it is difficult to prove that the entered data really comes from the driver. In other words, there has been fear that there may be attacks from a "man-in-the-middle".

[0004] Within the current development of legislation for smart tachograph version 2, an interface that makes it possible to create a tachograph HMI in external units, such as mobile phones, have been introduced. Hence, a wireless tachograph interface for external units, which is based on Bluetooth, has been standardised. The standardised solution includes a security mechanism which implies that the driver card shall be used in order to pair the external unit with the tachograph. It has also been suggested that vehicle ECUs can also, on voluntary basis, use this Bluetooth interface specification as well. However, this interface is not optimal for all situations.

Summary

[0005] It is an object of the disclosure to provide a solution that enables remote control of the tachograph from inside the cabin. It is a further object to provide a solution that is secure, user-friendly and protected from for external attacks.

[0006] According to a first aspect, the disclosure relates to a method for use in a control unit of a vehicle, for remotely controlling a tachograph arranged in the vehicle. The method comprises communicating a pairing request and a pairing accept between the tachograph and the control unit to enter a paired state 202 where a secure connection is established between the tachograph and the control unit. The method further comprises receiving, over the secure connection, a message identifying a driver card inserted in the tachograph, obtaining authentication data of a driver present in the vehicle, and authenticating the driver present in the vehicle by comparing the obtained authentication data with driver identity data of the inserted driver card obtained from a driver database. The method finally comprises performing the steps of sending, over the secure connection, a verification confirming successful authentication of the driver present in the vehicle and entering a remote-control state in which the control unit is enabled to remotely control the tachograph via the secure connection, in response to the authenticating being successful. Thereby, the tachograph can be controlled from a user interface device of the vehicle, such as by an in-vehicle display. It will typically be a better alternative for the driver to use the in-vehicle display than a remote device. Hence, the driver may have a more friendly interface for some of the basic tachograph functions without direct interaction with the tachograph. Furthermore, as the driver present is authenticated it is assured that it is the holder of the driver card that also controls the tachograph. Also, communication between the tachograph and the vehicle can take place over the CAN, which is typically more secure than using a wireless connection like Bluetooth.

[0007] In some embodiments the obtaining authentication data comprises obtaining biometric authentication data of the driver using a sensor device arranged in the vehicle. In some embodiments the obtaining authentication data comprises receiving authentication data received via a user interface device arranged in the vehicle. Hence, man in the middle attacks are avoided as the driver identity is verified using hardware arranged in the driver cabin, using for example biometric authentication.

[0008] In some embodiments the obtaining authentication data comprises obtaining a driver profile of the driver present in the vehicle from the driver database, and applying the obtained driver profile when operating the tachograph in the remote-control state. Hence, when a driver is identified, driver settings in the vehicle that has been stored earlier in the database may automatically be activated. This could be valuable if several drivers are using the same vehicle but have different settings.

[0009] In some embodiments the applying comprises one or more of customizing display layout or customizing language setting based on the obtained driver profile of the authenticated driver. Hence, a variety of options are available that may further improve user experience and driver safety.

[0010] In some embodiments the control unit is in the remote-control state enabled to perform one or more functions associated with the tachograph from a user interface device arranged in the vehicle. For example, the

control unit is enabled to add, update, or delete a driver profile of the authenticated driver from the driver database, provide input to tachograph, control the tachograph to perform actions, such as ejecting driver card or starting printing, and/or display tachograph data on a user interface device arranged in the vehicle. Thereby, the driver does not need to interact directly with the tachograph.

[0011] In some embodiments the driver database is stored in the vehicle or in the control unit. In some embodiments a certain user permission level is required to add new drivers to the driver database. Hence, information about drivers that are authorized to drive the vehicle can be stored on-board or off-board and controlled for example by a vehicle manufacturer.

[0012] In some embodiments the communicated pairing request and/or the paring accept comprises an authenticated confirmation enabling the tachograph and/or the control unit to authorize the pairing. This enables the tachograph or control unit to evaluate any pairing request. Hence, pairing with untrusted devices is avoided.

[0013] In some embodiments the authenticated confirmation proves that pairing is performed using a certified tachograph pairing software and/or that pairing is approved by a user holding the certain user permission level. Hence, pairing may only be done by trusted user's such as by the vehicle manufacturer or authorized workshops.

[0014] In some embodiments the method comprises evaluating, based on the authenticated confirmation, whether pairing is allowed and entering a paired state in response to the evaluating indicating that pairing is performed using a certified tachograph pairing software and/or that pairing is approved by a user holding the certain user permission level. Hence, pairing can be rejected if initiated by others than the vehicle manufacturer or authorized service stations.

[0015] In some embodiments the communicating comprises sending, over the secure connection, a pairing accept in response to the evaluating indicating that pairing is allowed. Hence, the tachograph is informed that pairing is completed.

[0016] In some embodiments the method comprises detecting a first trigger to exit the remote-control state and re-entering the paired state in response to detecting the first trigger. Hence, the remote state may be terminated for different reasons to avoid that the tachograph is remotely controlled when security is not confirmed.

[0017] In some embodiments the detecting the first trigger comprises one or more of receiving an instruction via a user interface device arranged in the vehicle, receiving, from the tachograph, a message indicating that a driver card has been removed, receiving a message from an off-board control device, and obtaining data, using a sensor arranged in the vehicle associated with driver presence in the vehicle. Hence, the remote control may be automatically terminated when the driver leaves the vehicle.

[0018] In some embodiments the method comprises sending an instruction, over the secure connection, to exit the remote-control state, in response to detecting the first trigger. The tachograph will then be informed such that the tachograph can also terminate the remote control.

[0019] In some embodiments the method comprises detecting a second trigger to exit the paired state entering an unpaired state in response to detecting the second trigger. Thereby, pairing may be terminated in different situations, for example when it is not secure to keep the pairing.

[0020] In some embodiments the detecting a second trigger comprises one or more of detecting interruption of the secure connection, receiving an instruction via a user interface device arranged in the vehicle, detecting expiry of a pairing timer, receiving message received from an off-board control device. Thereby, the pairing can be terminated when the connection is not verified or when a user, service centre or manufacturing instructs it. Hence, pairing may be terminated in situations when security is jeopardised.

[0021] In some embodiments the method comprises sending, over the secure connection, an instruction to exit the paired state, in response to detecting the second trigger. The tachograph will then be informed such that the tachograph can also enter the unpaired state.

[0022] According to a second aspect, the disclosure relates to a method for use in a tachograph arranged in a vehicle, for enabling remote control of the tachograph by a control unit of the vehicle. The method comprises communicating a pairing request and a paring accept between the tachograph and the control unit to enter a paired state where a secure connection is established between the tachograph and the control unit. The method also comprises sending a message identifying a driver card inserted in the tachograph over the secure connection and receiving, over the secure connection, a verification confirming successful authentication of a driver present in the vehicle. The method further comprises entering a remote-control state in which remote the control unit is enabled to remotely control the tachograph via the secure connection, in response to receiving the message.

[0023] According to a third aspect, the disclosure relates to a computer program comprising instructions which, when the program is executed by a computer, cause the computer to carry out the method according to the first or second aspect.

[0024] According to a fourth aspect, the disclosure relates to a computer-readable medium comprising instructions which, when executed by a computer, cause the computer to carry out the method according to the first or second aspect.

[0025] According to a fifth aspect, the disclosure relates to a control unit configured to perform the method according to any one of the embodiments according to the first aspect.

[0026] According to a sixth aspect, the disclosure re-

lates to a tachograph configured to perform the method according to any one of the embodiments according to the second aspect.

[0027] According to a seventh aspect, the disclosure relates to a vehicle comprising a tachograph according to the sixth aspect and/or the control unit according to the fifth aspect.

Brief description of the drawings

[0028]

Fig. 1 illustrates a truck where the proposed technique is implemented.

Fig. 2 illustrates a state machine of a connection between a control unit and a tachograph.

Fig. 3A and 3B illustrates signaling between a tachograph and a control unit arranged in a vehicle.

Fig. 4A and 4B are flow charts of the method for use in a control unit for remotely controlling a tachograph arranged in the vehicle according to the first aspect.

Fig. 5 illustrates a control unit according to the fourth aspect and connected devices in further detail.

Fig. 6 is a flowchart of the method, for use in a tachograph, for enabling remote control of the tachograph by a control unit of the vehicle according to the second aspect.

Detailed description

[0029] This disclosure is based on the insight that using a Bluetooth interface and a HMI originally intended for external devices, such as smartphones, may not be efficient to provide a good driver interface and working environment inside the cabin of a vehicle. Hence, this disclosure proposes solutions that further improve the driver interface and working environment for operating the tachograph from inside the cabin with maintained security.

[0030] More specifically, methods and devices are herein proposed that enable remote control of a tachograph from a control unit arranged in the vehicle, for example by a Digital Driver Unit, DDU, also known as the infotainment system and/or instrument cluster. The proposed concept is based on the insight that by utilizing hardware arranged in the vehicle, security of the remote control can be assured. More specifically, the inventors have realized that if the control unit and the tachograph are paired to establish security and trust, it is possible to use hardware of the vehicle to authenticate the user to access the tachograph.

[0031] In other words, the methods involves pairing the control unit and the tachograph, for example over the CAN. The pairing may be restricted such that it can only be performed by users having a certain competence, for example only by authorized service stations. After pairing a secure connection is established between the tachograph and the control unit. This secure connection is not tied to one particular driver or driver card, but may be reused by several drivers. The method further comprises authenticating, over the secure connection, a driver present in the vehicle, by comparing authentication data obtained using hardware in the vehicle with identity data corresponding to a driver card inserted in the tachograph. The driver is only allowed to control the tachograph from a user interface of the vehicle if such authentication is successful. However, no direct interaction between the driver and the tachograph, apart from inserting the driver card, is required. To assure that only authorized drivers are allowed to control the tachograph the method uses identity data stored in a driver database, which may be secure and/or anonym ized

[0032] In some embodiments, the authentication is based on fingerprint detection, facial recognition, or similar biometric identification as a way (in addition to PIN code) to obtain biometric information before the driver is allowed to remotely control the tachograph with the DDU. When remote control in enabled, the driver can use for example a touch screen of a display or wheel buttons of the dashboard to control the tachograph. As the authentication is controlled by a trusted vehicle authenticated and/or authorized by the pairing, security can be kept very high. Hence, the proposed method considers security aspects relating to both the authenticity of the driver, the driver card, and the hardware.

[0033] Fig. 1 illustrates a vehicle 1, more specifically a truck, where the proposed technique may also be implemented. The vehicle of Fig 1 is a manually operated vehicle 1. In some embodiments, the vehicle 1 is configured to be operated in an autonomous mode, where the vehicle can itself (e.g. under driver supervision) perform all driving tasks and monitor the driving environment. For simplicity only some parts of the vehicle 1 that are associated with the proposed method are shown in Fig. 1. Thus, the illustrated vehicle 1 of Fig. 1 comprises a control unit 10, a tachograph 20, a sensor device 30, a user interface device 40 and a driver database 50.

[0034] The vehicle 1 comprises a plurality of electrical systems and subsystems. For example, there are several Electrical Control Units, ECUs, connected to the vehicle controller area network, CAN. The tachograph 20 is one and the control unit 10 is another.

[0035] The control unit 10 is for example a DDU also known as the infotainment system and/or instrument cluster. The DDU is an ECU that controls instrumentation that is typically displayed with a digital readout rather than with the traditional analogue gauges. The control unit 10 is for example configured to control the user interface device 40. The user interface device 40 may comprise a display and a data input mechanism, typically a touch screen. Hence, the control unit 10 is configured to provide information to the driver and to receive input data

from the driver via the user interface device 40. The control unit is also configured to enable remote control of the tachograph 20 from the user interface device 40, as will be further explained in connection with the method of Fig. 4A and 4B.

[0036] The tachograph 20 is configured to measure the speed and driven distance, times (e.g. driving and resting time), position of the vehicle (e.g. using GNSS) and the driving status and driver's activities (e.g. driving/loading/unloading). The tachograph 20 typically also supports manual entry of data, for example specific conditions such as load/unload, start and end country, border crossing etc. may be manually entered. Tachographs also support manual entry of activity data such as work and resting time under controlled conditions. To drive a vehicle 1 equipped with a tachograph 20, a driver needs a driver card 21 (illustrated in Fig.5) to be allowed to drive this vehicle. The driver card 21 comprises a driver identity of a corresponding driver. Data recorded by the tachograph 20 is stored in internal memory and/or in the driver card 21. Data may also be displayed on a tachograph display or printed on paper. Furthermore, the tachograph 20 may detect events and faults and send warnings to the driver to warn about events and/or faults, such as that it is time to rest in accordance with national or regional regulations. The tachograph 20 is also configured to enable remote control of the tachograph 20 from the user interface device 40, as will be further explained in connection with the method of Fig.6.

[0037] As the control unit 10 and the tachograph 20 are separate units, they are typically produced by different suppliers. The control unit 10 and the tachograph 20 are configured to communicate over an interface, such as over the CAN. The control unit 10 and the tachograph 20 are typically provided by digital certificates that enables encryption and authentication. A digital certificate is an electronic document used to prove the ownership of a public key. Digital certificates typically include a certified public key, identifying information about the entity that owns the public key, metadata relating to the digital certificate and a digital signature of the public key created by the issuer of the certificate. The control unit 10 and the tachograph 20 may also be pre-configured by information about trusted units that they are allowed to connect to or to be paired with. For example, the tachograph may be pre-configured with a root certificate of a vehicle manufacturer, whereby it will consider all vehicles that have a certificate generated from this root certificate as trusted.

[0038] The sensor device 30 is configured to obtain biometric authentication data of the driver 2. The sensor device 30 is for example a camera configured to enable face or iris detection or similar. Alternatively, the sensor device 30 is a fingerprint sensor or other biometric sensor.

[0039] The driver database 50 comprises information about drivers that are authorized to drive the vehicle 1. For example, the driver database comprises driver name, driver card number, index of card number etc. The driver database 50 also comprises authentication data of the drivers, such as PIN codes or biometric info, that enables authentication. In some embodiments, the driver database 50 also comprises driver specific settings, such as for example, display layout and driver selected language. The driver specific settings enable the possibilities to have a nice and user-friendly environment for the driver when remotely controlling the tachograph.

[0040] The database 50 is typically associated with certain access restrictions. In other words, in some embodiments, a certain user permission level is required to add new drivers to the driver database 50. In other words, only trusted users are allowed to add users to the database. The permission level is for example granted on a certificate of a user. The permission is typically granted by a manufacturer of the vehicle 1 or similar, whereby access to the database 50 may be controlled. For example, only an authorized service station (holding a certain certificate) is allowed to add new drivers to the database. Once a driver is added to the data base 50 the driver may be allowed to edit her/his own profile. Typically, update of the database need to be done when the driver 2 has proved for the control unit 10 that it is the correct person who is in the driver seat. This is done either by biometric identification or PIN code and cross-referencing to the driver card ID number. In other words, in some embodiments an authenticated driver 2 is permitted to modify her/his own user profile.

[0041] In the illustrated embodiments, the driver database 50 is stored in the control unit 10. However, in alternative embodiments it is stored in elsewhere the vehicle 1 or off-board.

[0042] Fig. 2 is a state diagram illustrating different states of a connection between a control unit 10 and a tachograph 20. In other words, the connection will have a state, and consequently both the tachograph 20 and the control unit 10 will also be assigned this state. After installation, when the tachograph 20 and the control unit 10 are connected to the CAN the connection will typically be in an unpaired state 201, where no secure connection is established between the control unit 10 and tachograph 20. In this state the tachograph will not accept any (or only a few) remote-control requests that come from the control unit 10. In this mode the tachograph may send data to the control unit 10, but only data that does not require security.

[0043] To enable remote control pairing is required. Upon successful pairing, the connection will transition to a paired state 202, in which a secure connection has been established between the control unit 10 and the tachograph 20, but where remote control is not enabled, for example, because no driver card is inserted, or because the driver has not been authenticated. A secure connection is for example a connection that is encrypted by one or more security protocols to ensure the security of data flowing between two or more nodes. Alternatively, the connection is secure in the sense that both parties

are authenticated, whereby it is assured that information comes from the authenticated sender.

[0044] From the paired state 202 the connection may transition to a remote-control state 203 (also referred to as a remote display mode), where the control unit 10 is able to remotely control the tachograph 20. This is done when a driver card 21 is inserted in the tachograph 20 and the driver present in the cabin 3 (Fig. 1) is authenticated, as will be further described below. When the control unit 10 is in the remote-control state 203 the control unit 10 is enabled to perform one or more functions associated with the tachograph 20 from a user interface device 40 arranged in the vehicle 1. For example, the driver may provide input to tachograph 20, control the tachograph 20 to perform actions, such as ejecting driver card 21 or starting printing or displaying tachograph data on a user interface device 40 arranged in the vehicle 1. The display function may here include protected user information that was not shown in other states 201, 202.

[0045] In the remote-control state, the database 50 could possibly be reached from the user interface device 40. At least the driver 2 may be allowed to update her/his driver profile. For example, the driver may change language or layout. The driver may also be allowed to delete her/his driver profile from the driver database 50. For example, if the driver does not intend to drive the vehicle 1 anymore and does not want the biometric data to be stored in the database 50 for security reasons. The state of the connection may change back to the paired 202 or unpaired state 201, for example when a driver 2 leaves the vehicle 1 (and consequently removes the driver card 21) or due to security reasons that trigger unpairing.

[0046] The state transitions will now be further described below with reference to the signaling diagrams of Figs. 3A and 3B and the flow charts of Figs. 4A, 4B and 6. Fig. 3A and 3B illustrates signaling between a tachograph and a control unit 10 arranged in a vehicle. Fig. 4A and 4B are flow charts of the method for remotely controlling a tachograph arranged in the vehicle according to the first aspect. Fig. 6 is a flowchart of the method, for use in a tachograph 20, for enabling remote control of the tachograph 20 by a control unit 10 of the vehicle 1 according to the second aspect.

[0047] The proposed methods may be implemented as a computer program comprising instructions which, when the program is executed by a computer (e.g. a processor in the control unit 10 or tachograph 20), cause the computer to carry out the method. According to some embodiments the computer program is stored in a computer-readable medium (e.g. a memory or a compact disc) that comprises instructions which, when executed by a computer, cause the computer to carry out the method.

[0048] The first part of the proposed methods relates to pairing the control unit 10 and the tachograph 20. This corresponds to a state transition from the unpaired state 201 to the paired state 202. When the control unit 10 and the tachograph 20 are paired they communicate with each other through an established connection. This implies that the devices have verified each other's identity using for example certificate exchange, which excluded pairing with untrusted devices. Furthermore, the established connection may be encrypted, encoded or verified in any suitable manner, such that no external party can read or change data that is communicated.

[0049] Paring is typically initiated when either the control unit 10 or the tachograph 20 sends S11, S21 a pairing request. The communication between the tachograph 20 and the control unit 20, typically takes place over the CAN, which is more secure than a wireless interface. In this case, the pairing could be initiated either by the control unit 10 or by the tachograph 20. Hence the pairing request is either transmitted S21 by the control unit 10, or it is transmitted S11 by the tachograph 20. The other party then receives and evaluates S12, S22 the pairing request. Pairing is completed when a pairing accept is transmitted S13, S23. When pairing is completed the control unit 20 and the tachograph enters S14, S24 the paired state 202. In other words, the method for use in a control unit (Fig. 4A, 4B) comprises communicating S21, S23 a pairing request and a pairing accept between the tachograph 20 and the control unit 10 to enter a paired state 202 where a secure connection is established between the tachograph 20 and the control unit 10. Also the method for use in a tachograph (Fig. 6) comprises communicating S21, S23 a pairing request and a paring accept between the tachograph 20 and the control unit 10 to enter a paired state 202 where a secure connection is established between the tachograph 20 and the control unit 10. However, the pairing procedure may in addition involve exchanging further messages in addition to the pairing request and pairing accept depending on implementation.

[0050] Typically, pairing is performed by a manufacturer before the vehicle 1 is put into use. Alternatively, the pairing may the performed by an authorized service station, for example if the tachograph 20 is updated or exchanged. During the pairing procedure the control unit 10 and/or the tachograph 20 may want to ascertain that pairing is allowed. In other words, that it is initiated by someone that has authority or permission. Permission may be assigned to digital certificates. This may be achieved by including authentication or authorization information in the pairing request and/or in the pairing response (or in an intermediate message). The authentication information may be a signature or similar generated for example by certain software or a signature that is tied to a user identity, for example using a digital certificate that is granted the permission to perform tachograph pairing. The transition to the paired state may not occur until it is ascertained that pairing is allowed. Hence, in some embodiments the communicated pairing request and/or the paring accept comprises an authenticated confirmation enabling the tachograph 20 and/or the control unit 10 to authorize the pairing. The authentication may be a signature or symbol sequence or similar. The

authenticated confirmation proves that pairing is performed using a certified tachograph pairing software and/or that pairing is approved by a user holding the certain user permission level. In this way it is assured that the tachograph 20 is only paired by trusted control units 10.

[0051] In other words, in some embodiments the method for use in a control unit (Fig. 4A, 4B) comprises evaluating S22, based on the authenticated confirmation, whether pairing is allowed and entering S24 a paired state 202 in response to the evaluating S22 indicating that pairing is performed using a certified tachograph pairing software and/or that pairing is approved by a user holding the certain user permission level. In some embodiments the communicating comprises sending S23, over the secure connection, the pairing accept in response to the evaluating S22 indicating that pairing is allowed.

[0052] In the same way the method for use in a tachograph (Fig. 6) comprises evaluating S12, based on the authenticated confirmation, whether pairing is allowed and entering S14 a paired state 202 in response to the evaluating S12 indicating that pairing is performed using a certified tachograph pairing software and/or that pairing is approved by a user holding the certain user permission level. In some embodiments the communicating comprises sending S13, over the secure connection, the pairing accepts in response to the evaluating S12 indicating that pairing is allowed.

[0053] The control unit 10 and the tachograph 20 are now paired and trust is established. This means that the tachograph considers the vehicle as trusted. The second part of the proposed methods relates to verifying that the user that tries to control the tachograph 20 is actually a driver 2 present in the cabin 3 of the vehicle 1 and not someone else. The second part is for example initiated when a driver 2 inserts a driver card 21 in the tachograph 20. Hence, the method for use in a tachograph 20 (Fig. 6) comprises detecting S15 that a driver card 21 has been inserted and sending S16 a message identifying the driver card 21 inserted in the tachograph 20 over the secure connection. The method for use in a control unit (Fig. 4A, 4B) comprises receiving S25, over the secure connection, a message identifying a driver card 21 inserted in the tachograph 20. The message comprises for example a driver card identity or an identity number of the driver or any other information suitable to indicative of an identity of the driver 2.

[0054] Authentication of the driver 2 is then performed by the control unit 10 by using hardware in the vehicle 1. More specifically, the method for use in a control unit 10 (Fig. 4A, 4B) comprises obtaining S26 authentication data of a driver present in the vehicle 1. The authentication data may be either some data, for example a PIN, inserted using an input interface 40, such as a keyboard or touch screen. In other words, in some embodiments the obtaining S26 authentication data comprises receiving S26b authentication data received via a user interface device 40 arranged in the vehicle 1.

[0055] Alternatively, or in addition, biometric data may be used. In some embodiments the obtaining S26 authentication data comprises obtaining S26a biometric authentication data of the driver using a sensor device 30 arranged in the vehicle 1. The biometric data may be any feasible biometric data such as fingerprint data, face data, iris data.

[0056] The obtained authentication data is then compared with identity data stored in the data base 50. Hence, driver identity data corresponding to the driver identity received from the tachograph 20 is obtained S27 (i.e. retrieved or read out) from the database 50. For example, a PIN inserted by a driver is compared with a PIN stored in the database. Alternatively, a fingerprint provided by the driver present is compared with prerecorded user templates stored in the database 50. In other words, the method for use in a control unit 10 (Fig. 4A, 4B) comprises authenticating S28 the driver 2 present in the vehicle 1 by comparing the obtained authentication data with driver identity data of the inserted driver card obtained S27a from a driver database 50. In this way it is assured that the driver 2 present in the cabin 3 is the holder of the tachograph card 21 inserted in the tachograph 20.

[0057] In some embodiments, the database 50 comprises more data in addition to the user identity data. For example, a driver profile of the driver is stored. In other words, in some embodiments the method for use in a control unit 10 (Fig. 4A, 4B) comprises obtaining S27b a driver profile of the driver 2 present in the vehicle from the driver database 50.

[0058] If authentication is successful, the control unit 10 informs the tachograph and activates the remote control. If authentication is unsuccessful, the method stops. Possibly the control unit 10 informs the tachograph 20 about the authentication failure. In any case a message may be displayed on the user interface device 50 to inform the user about the outcome. In other words, the method for use in a control unit 10 (Fig. 4A, 4B) comprises in response to the authenticating S28 being successful, performing the steps of sending S29, over the secure connection, a verification confirming successful authentication of the driver 2 present in the vehicle and entering S210 a remote-control state 203 in which the control unit 10 is enabled to remotely control the tachograph via the secure connection. In the same way the method for use in a tachograph (Fig. 6) comprises receiving S17, over the secure connection, a verification confirming successful authentication of a driver 2 present in the vehicle, and entering S18, the remote-control state 203 in response to receiving S29 the message. Example functions that a driver may access when remote control is enabled are for example "manual entries" as defined in the tachograph legislation, starting a printout, eject driver card 21 from the tachograph 20 and so on.

[0059] When the remote control is enabled, a user interface of the tachograph is presented on a user interface

device 40 (for example a dashboard) of the vehicle 1. In some embodiments, the layout of the user interface can be customized based on a driver profile stored in the database 50. In other words, in some embodiments, the method for use in a control unit 10 (Fig. 4A, 4B) comprises applying S211 the obtained driver profile when operating the tachograph in the remote-control state. The applying S211 may comprise customizing display layout or customizing language setting based on the obtained driver profile of the authenticated driver. By storing driver specific settings in the database 50, it will be possible to add further functions in the future. These user settings are not limited to the tachograph.

[0060] The third part of the proposed methods (which continue in Fig. 3B, 4B) relates to exiting the remote-control state 203 or the paired state 202. This may be done for different reasons. In other words, there may be different triggers that causes the control unit 10 or tachograph 20 to determine that remote control shall be ended or to unpair the control unit 10 and the tachograph 20. In some cases, the reason is that the driver 2 has left the vehicle 1. In such a situation the connection will typically re-enter the paired state 202 until a new driver 2 arrives. In other situations, for example if a software conflict indicative of a security threat is discovered, the connection may re-enter the unpaired state 201 in order to interrupt all communication associated with sensitive information. Hence, in some embodiments, the method for use in a control unit 10 (Fig. 4A, 4B) comprises detecting S212 a first trigger to exit the remote-control state 203 and exiting S214 the remote-control state 203 response to detecting the first trigger.

[0061] The decision to terminate the remote-control due to the driver 2 leaving the vehicle 1 may be initiated by the tachograph 20. Hence, in some embodiments, the detected first trigger comprises receiving an instruction via a user interface device 40 arranged in the vehicle 1 or receiving S213, a message from the tachograph 20. The message indicates for example that a driver card 21 has been removed.

[0062] It is also possible that the absence of a driver 2 is detected by the vehicle 1 itself, for example based on sensor data. For example sensor data may indicate that the driver 2 has not been present for a predetermined amount of time or that another driver is identified who tries to use someone else's driver card. This might alone trigger the remote control to be interrupted immediately. In addition, a warning may be sent to an off-board system for security reasons. The off-board system may consider the driver card as "stolen" or "misused" and deletion of the driver from driver databases of other vehicles may be initiated. Hence, in some embodiments, the first trigger comprises obtaining data, using a sensor device 30 arranged in the vehicle 1 and associated with driver presence in the vehicle 1. The first trigger may also comprise receiving a message from an off-board control device 60, for example from an off-board control device 60, such as a manufacturer server, that the remote control shall be terminated.

[0063] If remote control is terminated by the control unit 10 the tachograph typically also has to be informed. Hence, in some embodiments, the method for use in a control unit 10 (Fig. 4A, 4B) comprises sending S213 an instruction, over the secure connection, to exit the remote-control state, in response to detecting S212 the first trigger. In the same way the method for use in a tachograph (Fig. 6) comprises receiving S19 an instruction, over the secure connection, to exit the remote-control state, and exiting S110, the remote-control state 203 in response to receiving S19 the message. The tachograph will then enter the paired state 202 or the unpaired state 201.

[0064] The remote control may also be terminated by the tachograph 20, for example by a user pushing a button on the tachograph 20. Hence, in some embodiments the second trigger comprises receiving S19 an instruction from the tachograph 20, to exit the paired state, and re-entering the unpaired state. In the same way the method for use in a tachograph (Fig. 6) comprises sending S216 an instruction, over the secure connection, to exit the paired state, and re-entering the unpaired state.

[0065] The connection may also be triggered to exit the paired state 202. Hence, in some embodiments, the method for use in a control unit 10 (Fig. 4A, 4B) comprises detecting S215 a second trigger to exit the paired state 202 entering S217 the unpaired state 202 in response to detecting the second trigger. The second trigger comprises for example detecting interruption of the secure connection or detecting expiry of a pairing timer. These triggers may indicate that the connection is not secure, for example there may be an attack from a man in the middle or someone is trying to manipulate the tachograph 20.

[0066] In some embodiments the second trigger comprises receiving message received from an off-board control device 60. For example, a manufacturer or other external party has discovered a possible attack or other security risk and therefore the connection should be interrupted and re-established.

[0067] The unpairing may also be initiated by a user. Hence, in some embodiments the second trigger comprises receiving an instruction via a user interface device 40 arranged in the vehicle 1.

[0068] If pairing is ended by the control unit 10 the tachograph 20 typically also has to be informed. Hence, in some embodiments, the method for use in a control unit 10 (Fig. 4A, 4B) comprises sending S216, over the secure connection, an instruction to exit the paired state 202, in response to detecting S215 the second trigger. In the same way the method for use in a tachograph (Fig. 6) comprises receiving S111 an instruction, over the secure connection, to exit the paired state, and re-entering S112, the unpaired state 201 in response to receiving S111 the message.

[0069] The unpairing may also be initiated by the tachograph 20, for example using a button on the tachograph

20. Hence, in some embodiments the second trigger comprises receiving S111 an instruction from the tachograph. In the same way the method for use in a tachograph (Fig. 6) comprises sending S216 an instruction, over the secure connection, to exit the paired state, and re-entering the unpaired state.

[0070] Fig. 5 illustrates a control unit 10 according to the fourth aspect in more detail and connected devices. In some embodiments, the control unit 10 is a "unit" in a functional sense. Hence, in some embodiments the control unit 10 is a control arrangement comprising several physical control units (for example several ECUs) that operate in corporation.

[0071] Hence, the control unit 10 comprises one or more ECUs. An ECU is basically a digital computer that controls one or more electrical systems (or electrical sub systems) of the vehicle 1 based on e.g. information read from sensors 13 and meters 14 placed at various parts and in different components of the vehicle 1. ECU is a generic term that is used in automotive electronics for any embedded system that controls one or more functions of the electrical system or sub systems in a transport vehicle. The vehicle 1 typically comprises a plurality of ECUs that communicate over a Controller Area Network, CAN, which in the future might be replaced by for example ethernet based solutions. In some embodiments, at least some parts of the control unit 10 are implemented off-board.

[0072] The control unit 10, or more specifically the processor 101 of the control unit 10, is configured to cause the control unit 10 to perform all aspects of the method for use in a control unit 10 described above and below. This is typically done by running computer program code stored in the data storage or memory 102 in the processor 101 of the control unit 10. The data storage 102 may also be configured to store semi-static vehicle parameters such as vehicle dimensions.

[0073] The control unit 10 may also comprise a communication interface 103 for communicating with other control units of the vehicle and/or with external systems. For example, the communication interface comprises a CAN bus and a wireless communication interface (such as a modem) using standard wireless and telecommunication techniques e.g. protocols standardized by 3GPP. The communication interface enables communication with the tachograph 20, the sensor device 30, the user interface device 40 and the database (if not included in the control unit 10), typically over the CAN bus. The communication interface may also be configured to enable communication with an off-board control device 60.

[0074] The terminology used in the description of the embodiments as illustrated in the accompanying drawings is not intended to be limiting of the described method, control unit or computer program. Various changes, substitutions and/or alterations may be made, without departing from disclosure embodiments as defined by the appended claims.

[0075] The term "or" as used herein, is to be interpreted as a mathematical OR, i.e., as an inclusive disjunction; not as a mathematical exclusive OR (XOR), unless expressly stated otherwise. In addition, the singular forms "a", "an" and "the" are to be interpreted as "at least one", thus also possibly comprising a plurality of entities of the same kind, unless expressly stated otherwise. It will be further understood that the terms "includes", "comprises", "including" and/ or "comprising", specifies the presence of stated features, actions, integers, steps, operations, elements, and/ or components, but do not preclude the presence or addition of one or more other features, actions, integers, steps, operations, elements, components, and/ or groups thereof. A single unit such as e.g. a processor may fulfil the functions of several items recited in the claims.

Claims

1. A method for use in a control unit (10) of a vehicle (1), for remotely controlling a tachograph (20) arranged in the vehicle (1), the method comprising:

   - communicating (S21, S23) a pairing request and a pairing accept between the tachograph (20) and the control unit (10) to enter a paired state (202) where a secure connection is established between the tachograph (20) and the control unit (10),
   - receiving (S25), over the secure connection, a message identifying a driver card (21) inserted in the tachograph (20),
   - obtaining (S26) authentication data of a driver present in the vehicle (1),
   - authenticating (S28) the driver (2) present in the vehicle (1) by comparing the obtained authentication data with driver identity data of the inserted driver card obtained (S27) from a driver database (50), and

   in response to the authenticating (S28) being successful, performing the steps of:

   - sending (S29), over the secure connection, a verification confirming successful authentication of the driver (2) present in the vehicle and
   - entering (S210) a remote-control state (203) in which the control unit (10) is enabled to remotely control the tachograph via the secure connection.

2. The method according to claim 1, wherein the obtaining (S26) authentication data comprises one or more of:

   - obtaining (S26a) biometric authentication data of the driver using a sensor device (30) arranged in the vehicle (1),

- receiving (S26b) authentication data received via a user interface device (40) arranged in the vehicle (1).

3. The method according to claim 1 or 2, comprising:

- obtaining (S27b) a driver profile of the driver (2) present in the vehicle from the driver database (50), and applying (S211) the obtained driver profile when operating the tachograph in the remote-control state (203).

4. The method of claim 3, where in the applying (S211) comprises one or more of customizing display layout customizing language setting based on the obtained driver profile of the authenticated driver.

5. The method according to any one of the preceding claims, wherein when the control unit (10) is in the remote-control state (203) the control unit (10) is enabled to perform one or more of the following functions associated with the tachograph (20) from a user interface device (40) arranged in the vehicle:

- providing input to tachograph (20),
- controlling the tachograph (20) to perform actions, such as ejecting driver card or starting printing,
- displaying tachograph data on a user interface device (40) arranged in the vehicle,
- adding or updating a driver profile of the authenticated driver stored in the driver database (50), and
- delete a driver profile of the authenticated driver from the driver database (50).

6. The method according to any one of the preceding claims, wherein the driver database (50) is stored in the vehicle (1) or in the control unit (10).

7. The method according to claim 6, wherein a certain user permission level is required to add new drivers to the driver database (50).

8. The method according to any one of the preceding claims, wherein the communicated pairing request and/or the pairing accept comprises an authenticated confirmation enabling the tachograph (20) and/or the control unit (10) to authorize the pairing,
wherein the authenticated confirmation proves that pairing is performed using a certified tachograph pairing software and/or that pairing is approved by a user holding the certain user permission level.

9. The method according to claim 8, comprising:

- evaluating (S22), based on the authenticated confirmation, whether pairing is allowed and entering (S24) a paired state (202) in response to the evaluating (S22) indicating that pairing is performed using a certified tachograph pairing software and/or that pairing is approved by a user holding the certain user permission level.

10. The method according to claim 9, comprising:

- wherein the communicating (S13, S23) comprises sending (S23), over the secure connection, a pairing accept in response to the evaluating (S22) indicating that pairing is allowed.

11. The method according to any one of the preceding claims comprising:

- detecting (S212) a first trigger to exit the remote-control state (203)
- and exit the remote-control state (203) in response to detecting the first trigger.

12. The method of claim 11, wherein the detecting (S212) the first trigger comprises one or more of:

- receiving an instruction via a user interface device (40) arranged in the vehicle,
- receiving (S213), from the tachograph, a message indicating that a driver card has been removed,
- receiving a message from an off-board control device (60), and
- obtaining data, using a sensor arranged in the vehicle associated with driver presence in the vehicle.

13. The method according to any one of the preceding claims comprising:

- detecting (S215) a second trigger to exit the paired state (202) and
- exiting the paired state (202) in response to detecting the second trigger.

14. The method of claim 13, wherein the detecting a second trigger (S215) comprises one or more of:

- detecting interruption of the secure connection,
- receiving an instruction via a user interface device (40) arranged in the vehicle (1),
- detecting expiry of a pairing timer,
- receiving message received from an off-board control device (60).

15. A computer program comprising instructions which, when the program is executed by a computer, cause the computer to carry out the method of any one of the claims 1 to 14.

16. A computer-readable storage medium comprising instructions which, when executed by a computer, cause the computer to carry out the method of any one of the claims 1 to 14.

17. A control arrangement configured to perform the method according to any one of claims 1 to 14.

18. A method for use in a tachograph (20) arranged in a vehicle (1), for enabling remote control of the tachograph (20) by a control unit (1) of the vehicle (1), the method comprising:

- communicating (S21, S23) a pairing request and a paring accept between the tachograph (20) and the control unit (10) to enter a paired state (202) where a secure connection is established between the tachograph (20) and the control unit (10),
- sending (S16) a message identifying a driver card (21) inserted in the tachograph (20) over the secure connection,
- receiving (S17), over the secure connection, a verification confirming successful authentication of a driver (2) present in the vehicle, and
- entering (S18), in response to receiving (29) the message, a remote-control state (203) in which remote the control unit (10) is enabled to remotely control the tachograph via the secure connection.

19. A vehicle (1) comprising the control unit (10) according to claim 1 to 14 and/or a tachograph (20) configured to perform the method according to claim 18.

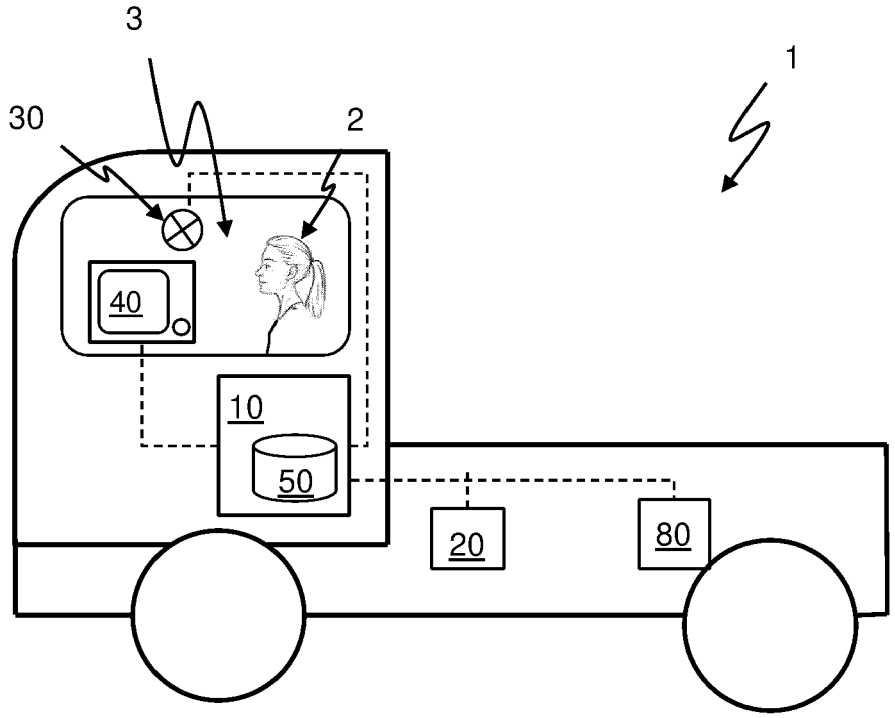
3
1
30
2
40
10
50
20
80

FIG. 1

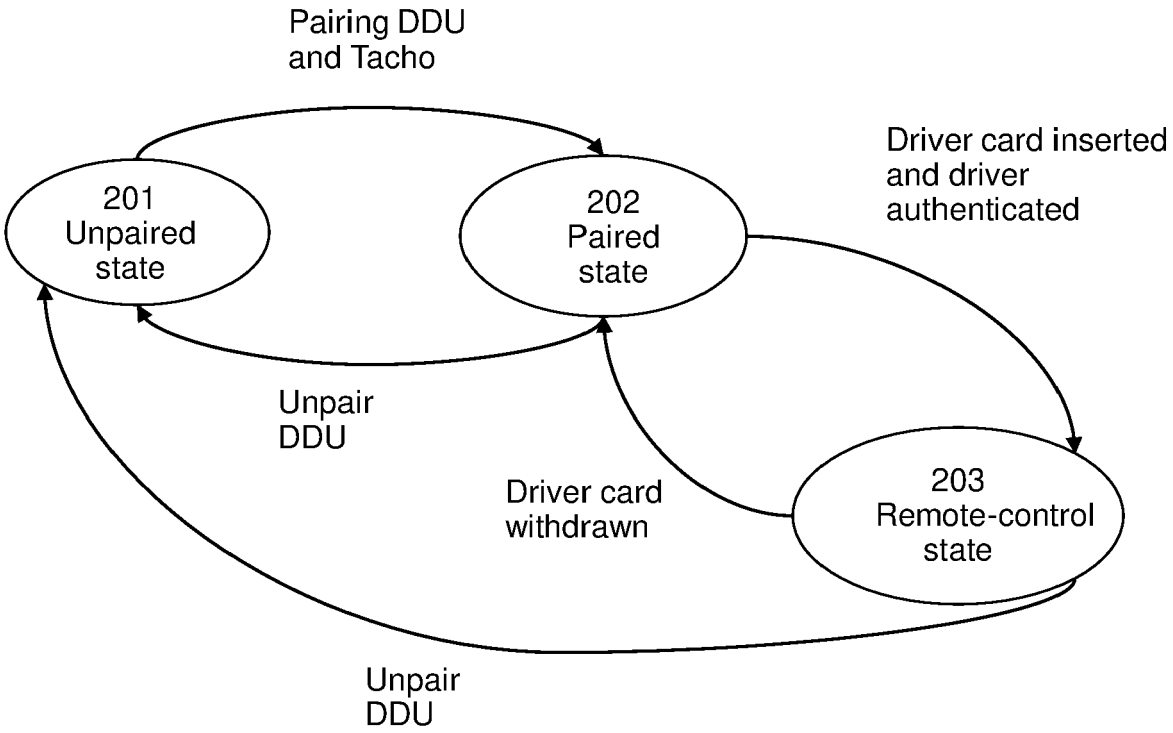
Pairing DDU
and Tacho
201
Unpaired
state
202
Paired
state
Driver card inserted
and driver
authenticated
Unpair
DDU
Driver card
withdrawn
203
Remote-control
state
Unpair
DDU

FIG. 2

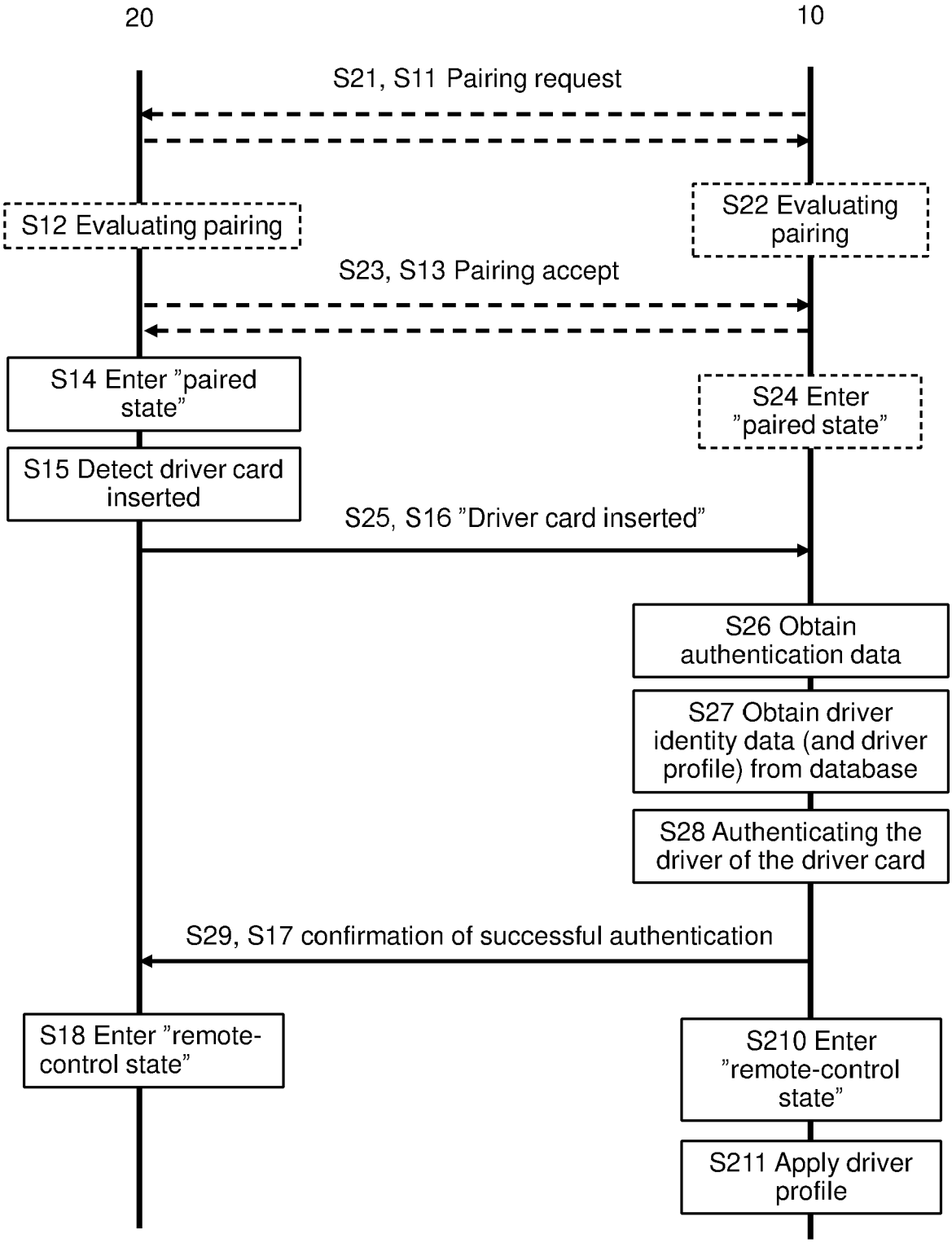
20
10
S21, S11 Pairing request
S12 Evaluating pairing
S22 Evaluating pairing
S23, S13 Pairing accept
S14 Enter "paired state"
S24 Enter "paired state"
S15 Detect driver card inserted
S25, S16 "Driver card inserted"
S26 Obtain authentication data
S27 Obtain driver identity data (and driver profile) from database
S28 Authenticating the driver of the driver card
S29, S17 confirmation of successful authentication
S18 Enter "remote-control state"
S210 Enter "remote-control state"
S211 Apply driver profile

Fig. 3A

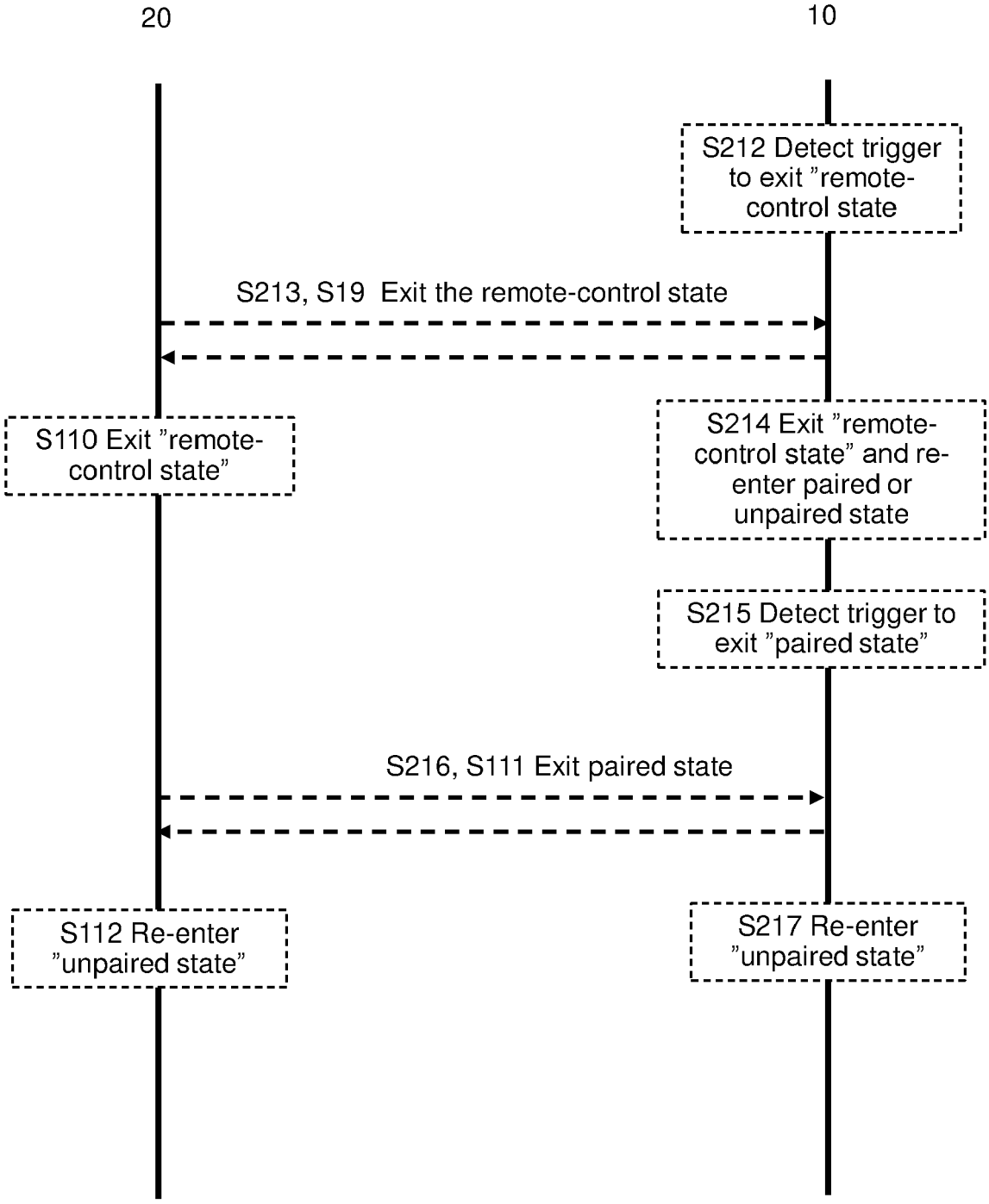
20
10
S212 Detect trigger to exit "remote-control state
S213, S19 Exit the remote-control state
S110 Exit "remote-control state"
S214 Exit "remote-control state" and re-enter paired or unpaired state
S215 Detect trigger to exit "paired state"
S216, S111 Exit paired state
S112 Re-enter "unpaired state"
S217 Re-enter "unpaired state"

Fig. 3B

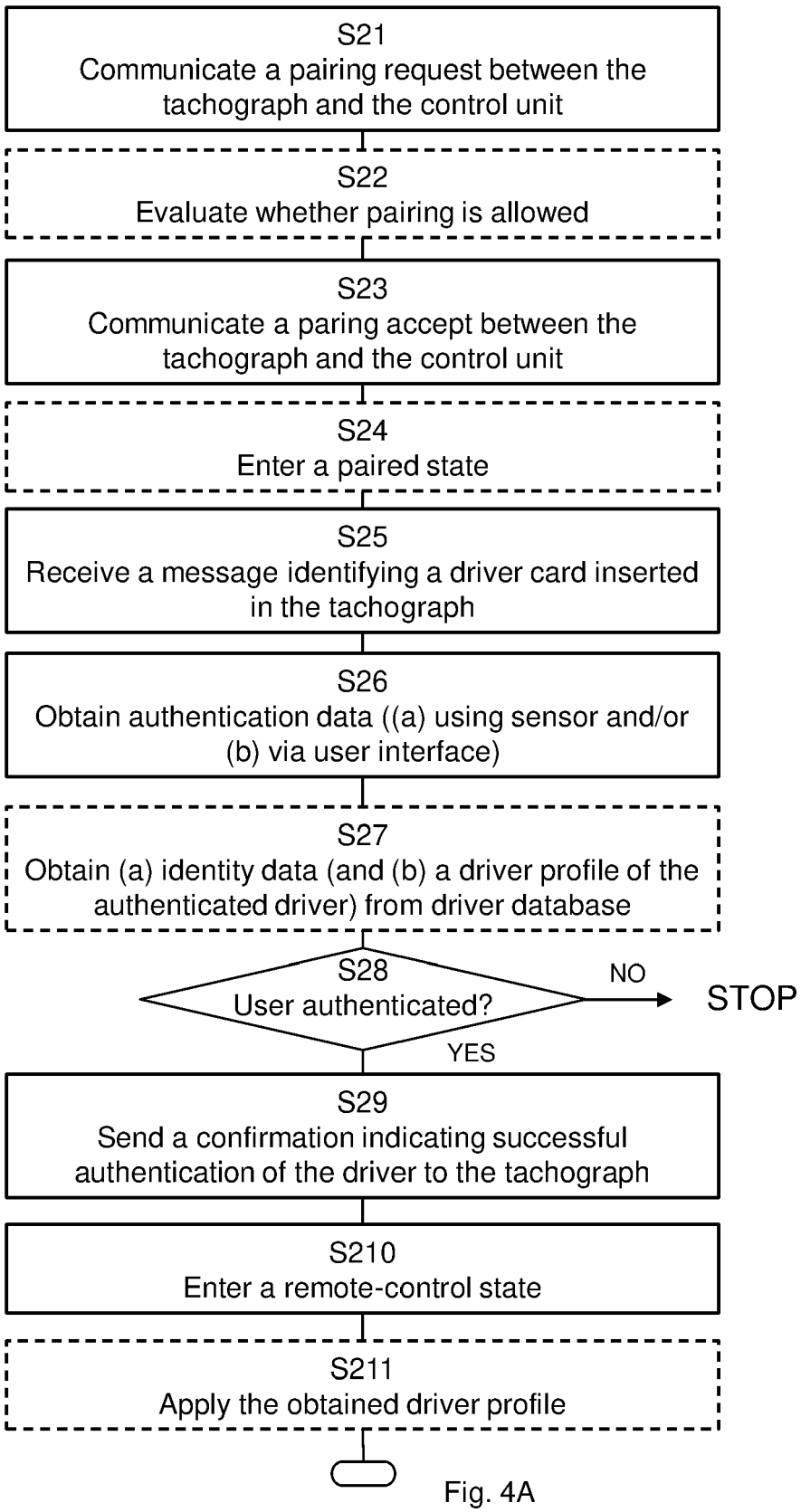
S21
Communicate a pairing request between the tachograph and the control unit
S22
Evaluate whether pairing is allowed
S23
Communicate a paring accept between the tachograph and the control unit
S24
Enter a paired state
S25
Receive a message identifying a driver card inserted in the tachograph
S26
Obtain authentication data ((a) using sensor and/or (b) via user interface)
S27
Obtain (a) identity data (and (b) a driver profile of the authenticated driver) from driver database
S28
User authenticated?
NO
STOP
YES
S29
Send a confirmation indicating successful authentication of the driver to the tachograph
S210
Enter a remote-control state
S211
Apply the obtained driver profile

Fig. 4A

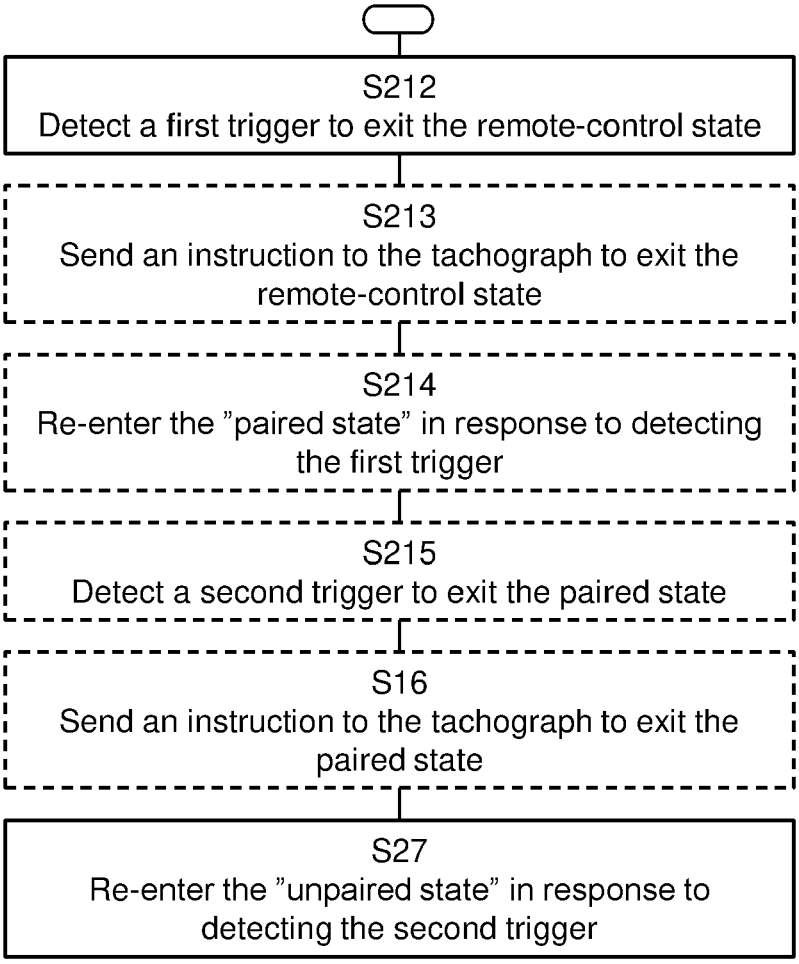
S212
Detect a first trigger to exit the remote-control state
S213
Send an instruction to the tachograph to exit the remote-control state
S214
Re-enter the "paired state" in response to detecting the first trigger
S215
Detect a second trigger to exit the paired state
S16
Send an instruction to the tachograph to exit the paired state
S27
Re-enter the "unpaired state" in response to detecting the second trigger

Fig. 4B

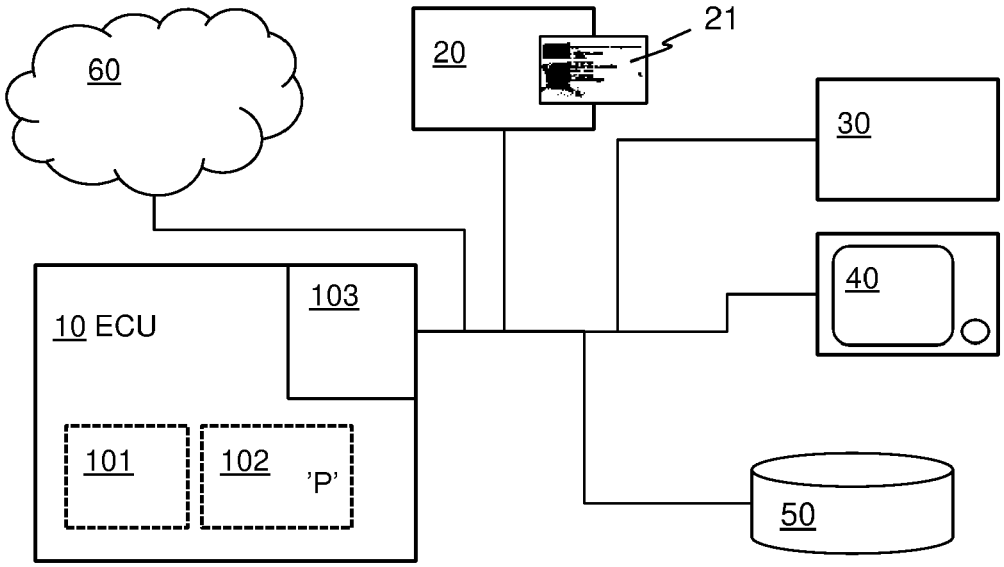
60
20
21
30
40
10 ECU
103
101
102
'P'
50

FIG. 5

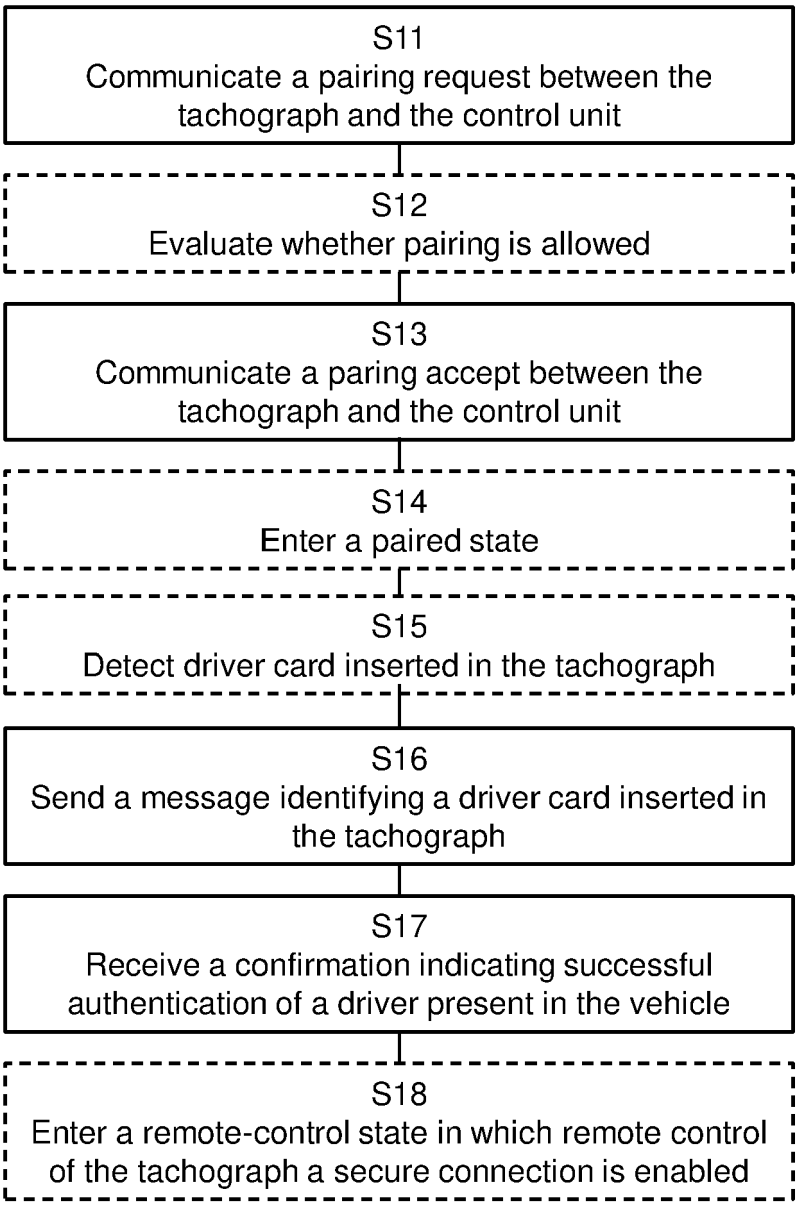
S11
Communicate a pairing request between the tachograph and the control unit
S12
Evaluate whether pairing is allowed
S13
Communicate a paring accept between the tachograph and the control unit
S14
Enter a paired state
S15
Detect driver card inserted in the tachograph
S16
Send a message identifying a driver card inserted in the tachograph
S17
Receive a confirmation indicating successful authentication of a driver present in the vehicle
S18
Enter a remote-control state in which remote control of the tachograph a secure connection is enabled

Fig. 6

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 22 18 2196

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	US 2008/244735 A1 (CALLENRYD FREDRIK [SE] ET AL) 2 October 2008 (2008-10-02) * abstract; figures 1A, 1B, 2 * * paragraph [0002] - paragraph [0057] *	1,3-19 2	INV. G07C5/08
A	Anonymous: "Appendix 13 (ITS Interface) of Commission Implementing Regulation (EU) 2016/799 - consolidated text version 26-02-2020", >M1 Commission Implementing Regulation) 02016R0799 - EN - 26, 26 February 2020 (2020-02-26), pages 31022020-2001, XP055977646, Retrieved from the Internet: URL:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0799-20200226&from=EN [retrieved on 2022-11-03] * the whole document *	1-19	
Y A	GB 2 426 363 A (DIGY HOLDINGS LTD [GB]; BALIUS SYSTEMS LTD [GB]) 22 November 2006 (2006-11-22) * page 12, line 18 - page 12, line 32 *	2 1,3-19	TECHNICAL FIELDS SEARCHED (IPC) G07C

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	4 November 2022	Holzmann, Wolf

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 22 18 2196

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.

04-11-2022

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008244735 A1	02-10-2008	BR PI0618547 A2	06-09-2011
		CN 101310309 A	19-11-2008
		EP 1952361 A1	06-08-2008
		SE 528774 C2	13-02-2007
		US 2008244735 A1	02-10-2008
		WO 2007058607 A1	24-05-2007
GB 2426363 A	22-11-2006	GB 2426363 A	22-11-2006
		WO 2006123159 A2	23-11-2006

EPO FORM P0459

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