(12) STANDARD PATENT (11) Application No. **AU 2012200542 B2**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Method for validating a road traffic control transaction

(51) International Patent Classification(s)
G08G 1/017 (2006.01) ***H04L 9/14*** (2006.01)

(21) Application No: **2012200542** (22) Date of Filing: **2012.01.31**

(30) Priority Data

(31) Number	(32) Date	(33) Country
11450041.6	**2011.03.22**	**EP**

(43) Publication Date: **2012.10.11**
(43) Publication Journal Date: **2012.10.11**
(44) Accepted Journal Date: **2013.10.31**

(71) Applicant(s)
Kapsch TrafficCom AG

(72) Inventor(s)
Hafenscher, Albert

(74) Agent / Attorney
FB Rice, Level 23 44 Market Street, SYDNEY, NSW, 2000

(56) Related Art
US 5898779 A
EP 2088568 A2

2012200542 31 Jan 2012

Abstract

Method for Validating a
Road Traffic Control Transaction

The invention pertains to a method for validating a road traffic control transaction (tr) that is generated by recording an image (pic) of a vehicle (7) in a control station (TE) of a road traffic control system (1) and reading an identification (9) of the vehicle (7) by means of OCR, wherein said control transaction is then sent to a transaction receiver (CI), and wherein said method comprises the following steps:

recording an image (pic) of the vehicle (7), reading a vehicle identification (9) in the recorded image (pic) by means of OCR and generating a control transaction (tr) thereof;

generating a random key (rd) and encrypting the recorded image (pic) into authentication data (au) with the random key (rd) and a cryptographic key (tk) of the transaction receiver (CI) in a separate processing element (AE) of the control station (TE);

sending the recorded image (pic), the control transaction (tr), the random key (rd) and the authentication data (au) to the transaction receiver (CI);

in the transaction receiver: encrypting the recorded image (pic) into nominal authentication data (au_r) with the received random key (rd) and the cryptographic key (tk) and

comparing the received authentication data (au) with the nominal authentication data (au_r),

wherein the control transaction (tr) is validated if the two datasets are identical.

(Fig. 3)

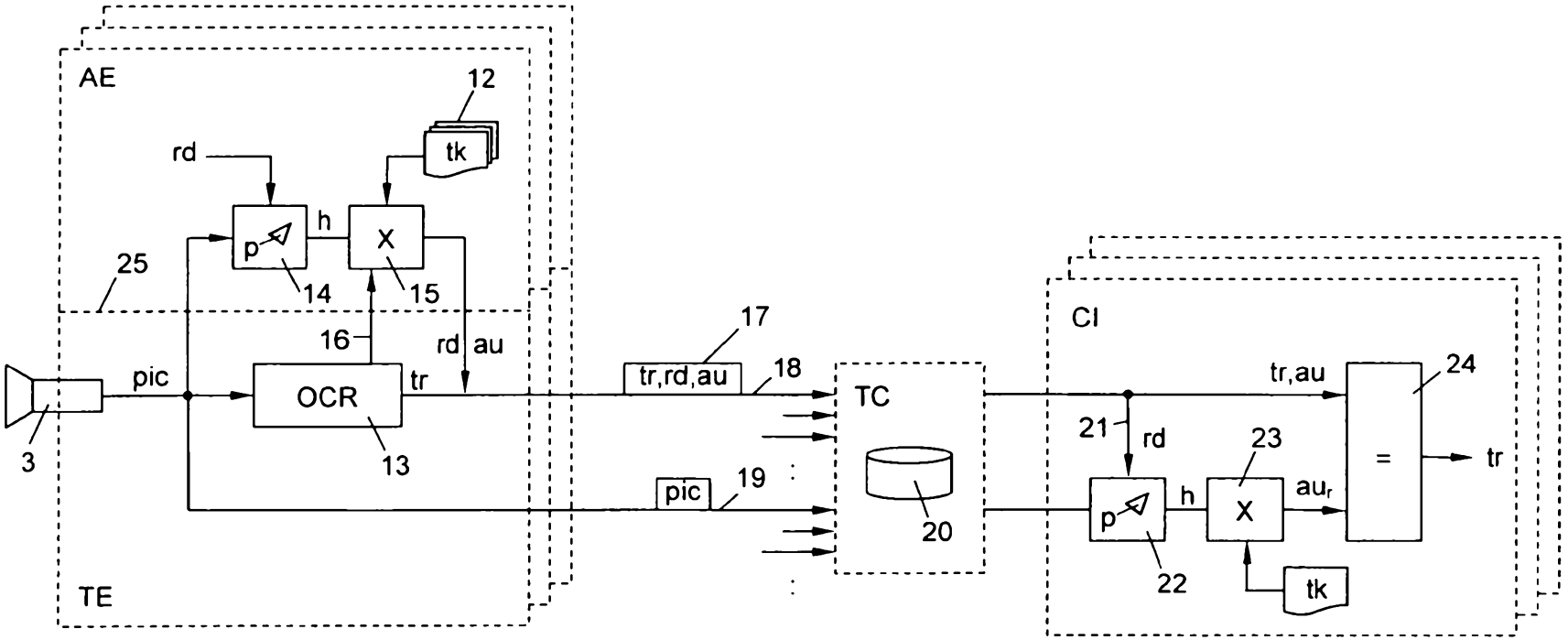
AE
12
tk
rd
h
p
X
14
15
25
16
rd
au
pic
OCR
tr
13
3
TE
17
tr,rd,au
18
pic
19
TC
20
CI
tr,au
24
21
rd
23
=
tr
p
h
X
au_r
22
tk

Fig. 3

2012200542 31 Jan 2012

AUSTRALIA

Patents Act 1990

KAPSCH TRAFFICCOM AG

COMPLETE SPECIFICATION
STANDARD PATENT

Invention Title:

Method for validating a road traffic control transaction

The following statement is a full description of this invention including the best method of performing it known to us:-

2012200542 31 Jan 2012

Method for Validating a Road Traffic Control Transaction

The present invention pertains to a method for validating a road traffic control transaction that is generated by recording an image of a vehicle in a control station of a road traffic control system and reading an identification of the vehicle in the recorded image by means of OCR, wherein said control transaction is then sent to a transaction receiver of the road traffic control system.

Road traffic control systems of this type are also referred to as "video control systems" because the control transactions are based on video recordings of the traffic at a control station. The systems can be used for various control purposes such as, e.g., for controlling the presence of a vehicle in a certain locality in order to calculate the fee for using this locality in the form of a road toll, zone toll or parking fee, for evidence purposes in the enforcement of speed limits or other traffic violations, for monitoring the compliance with hazardous materials transport regulations, the proper execution of winter road maintenance or street cleaning assignments, fleet vehicles entering and exiting business premises or rental cars entering and exiting car rental facilities, etc.

In this case, the vehicles are identified based on an optical character recognition (Optical Character Recognition, OCR) of the vehicle identification in the recorded images. In practice, the operator of the road traffic control system (in a road toll system: the "Toll Charger," TC) is not the same entity as the recipient and processor of the control transactions, usually the owner of the road traffic control system or a state agency ("Contract Issuer," CI). For the latter, the validation of the control transactions received from the operator with respect to legitimacy or authenticity is of decisive importance in order to prevent transactions that did not take place from being billed, charged or attributed to the users or persons liable to control.

EP 2 088 568 discloses a control station that prepares an electronic document with other vehicle recordings and with additional data, e.g. a vehicle identification read by means of OCR or the detected vehicle type, in case of a violation. Before the thusly prepared document is sent to the central office via a possibly insecure communication link, it is signed in accordance with a conventional private-public-key process. Although this makes it possible to detect a manipulation on the transmission link, a validation or authentication of the entire control transaction including the document preparation cannot be achieved in this way such that each of the control stations needs to be elaborately secured with additional sensor systems.

2012200542 23 Aug 2013

Any discussion of documents, acts, materials, devices, articles or the like which has been included in the present specification is not to be taken as an admission that any or all of these matters form part of the prior art base or were common general knowledge in the field relevant to the present invention as it existed before the priority date of each claim of this application.

Throughout this specification the word "comprise", or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated element, integer or step, or group of elements, integers or steps, but not the exclusion of any other element, integer or step, or group of elements, integers or steps.

According to the present invention, there is provided a method for validating a road traffic control transaction that is sent from a control station of a road traffic control system to a transaction receiver of the road traffic control system in the transaction receiver, including the following steps:

storing a cryptographic key assigned to the transaction receiver in the transaction receiver and in a separate processing element of the control station;

recording an image of a vehicle, reading an identification of the vehicle in the recorded image by means of OCR and generating a control transaction thereof in the control station;

generating a random key which defines an image section in the recorded image and encrypting the recorded image into authentication data with the random key and the cryptographic key in the separate processing element by the processes

-extracting the image section from the recorded section;

-forming a first hash value of the image section; and

-encrypting the first hash value with the cryptographic key into the authentication data;

sending the recorded image, the control transaction, the random key and the authentication data to the transaction receiver;

in the transaction receiver: encrypting the received recorded image into nominal authentication data with the received random key and the stored cryptographic key by the same process as conducted in the processing element; and

comparing the received authentication data with the nominal authentication data,

wherein the received control transaction is validated if the two datasets are identical.

The method enables the transaction recipient (contract issuer) to check control transactions and to reject unauthenticated control transactions directly at the interface with the control system operator such as, e.g., a toll system operator (toll charger). The

method utilises a separate processing element that is trusted by the transaction receiver and consequently provided with a cryptographic key of the transaction receiver in the control station. Authentication data for the transaction receiver is generated in connection with a random key of the control station that is unique to each transaction or recorded image and enables the transaction receiver to validate the original control

transaction based on the originally recorded image - by checking the authentication data in an autarkic fashion on its end.

The aforementioned control station may be realized stationary or mobile, feature one or more cameras and also have geographically distributed components such as, for example, a remote proxy computer for the OCR evaluation of the vehicle identification.

According to a preferred embodiment of the invention, several cryptographic keys assigned to different transaction receivers are stored in the processing element and the cryptographic key to be respectively used is selected in dependence on the vehicle identification read by means of OCR. In this way, control transactions for various transaction recipients such as, e.g., different agencies, police, fire department, road maintainer, etc., respectively can be individually authenticated directly at their origin and then validated.

The authentication data and the random key preferably are sent to the transaction receiver together with the control transaction such that the control transaction directly carries along the data that allows its validation. Alternatively, the authentication data and the random key may also be sent to the transaction receiver together with the recorded image, wherein corresponding references to the control transaction are provided in this case.

According to another particularly preferred embodiment of the invention, the random key defines an image section in the recorded image and the aforementioned encryption of the recorded image with the random key comprises the step of extracting the image section from the recorded image and the step of forming a first hash value of the image section. Consequently, it suffices to provide the processing element with an extremely low computing power because the encryption taking place therein is, as far as the random key is concerned, limited to the extraction of a random image section from the recorded image and the formation of a hash value thereof. The extraction of an image section reduces the data volume significantly and the formation of a hash value is a very simple computational process. The aforementioned hash value therefore is already available in the form of a significantly reduced input dataset for the further encryption with the cryptographic key, wherein any encryption method known from the pertinent technology can be applied with minimal effort.

The extracted image section preferably also contains the identification of the vehicle such that the validation security is increased.

It is particularly advantageous if this second encryption is also carried out with the aid of a hash value formation, i.e., the aforementioned encryption of the recorded image with the cryptographic key comprises the step of forming a second hash value of

the first hash value and the cryptographic key, wherein the second hash value then represents the authentication data.

The aforementioned image section may consist of any part of the recorded image that can be defined by the random key. For example, the random key defines the corner points of a peripheral contour that encloses a flat image section. Alternatively, the random key could define color values for image pixels and all image pixels with these color values jointly form the aforementioned image section.

In the context of the present description, the term "formation of a hash value" refers to the application of a practically irreversible n:1 transformal function to the input value, i.e., a function that is only reversible in an (extremely) ambiguous fashion, such that knowledge of the hash value practically makes it impossible to deduce the initial value (in this case: the image section). Examples of such hash functions are the checksum function, the modulo function, etc.

In other advantageous embodiments of the invention, a time stamp, an identification of the control station, an identification of the processing element and/or a serial count value may be integrated into the authentication data. Each of these specifications can be used for subsequent plausibility checks and therefore increases the security of the validation.

It is furthermore possible to store several cryptographic keys with assigned key identifications in the transaction receiver and in the processing element, as well as to integrate the key identification of the key used into the authentication data and to use the integrated key identification for determining the assigned key in the transaction receiver. This can also increase the security of the system.

The processing element that serves as authentication unit may consist of a software element, as well as a hardware element. It is preferred to use a hardware element that is connected to the control station via a physical interface, e.g., like a cryptographically secured hardware module (Secure Access Module, SAM), a USB-Token, etc. In this respect, it would preferably also be conceivable that the separation of the interface renders the hardware element unusable in order to prevent manipulations and to provide improved protection of confidence for the transaction receiver.

According to another preferred characteristic of the invention, the supplemented control transaction is sent from the control station to the transaction receiver via a first channel and the recorded image is sent from the control station to the transaction receiver via a second channel, wherein the supplemented control transaction and the corresponding recorded image are assigned to one another in the transaction receiver

with the aid of at least one mutual reference provided therein. Consequently, it is not absolutely imperative that the control transactions and the recorded images arrive simultaneously at the transaction receiver; for example, the recorded images could be stored in databases and made available to the transaction receiver for validation purposes in this form.

The invention is described in greater detail below with reference to one exemplary embodiment that is illustrated in the attached drawings. In these drawings,

Figure 1 shows a block diagram of an exemplary road traffic control system according to the invention in the form of an interoperable road toll system;

Figure 2 schematically shows one of the control stations of the road toll system according to Figure 1; and

Figure 3 shows a signal flow chart of the inventive method for validating control transactions within the road toll system according to Figure 1.

According to Figure 1, control transactions tr are generated by a plurality of different control stations (in this case: Tolling Entities) TE in an interoperable road traffic control system, in this case a road toll system 1, and sent to transaction recipients CI (Contract Issuers) for processing and/or billing purposes via operator-specific central offices (in this case: Toll Chargers) TC. Transaction receivers CI can receive control transactions tr from various central offices TC of the operator and these can in turn be connected to a plurality of different control stations TE, one of which is illustrated in an exemplary fashion in Figure 2.

The control station TE according to Figure 2 comprises an optional radio beacon 2 that operates, e.g., in accordance with the DSRC (Dedicated Short Range Communication) standard or the WAVE (Wireless Access in a Vehicle Environment) standard and a photo or video camera 3, wherein the radio beacon and the photo or video camera are connected to a station computer 4 that, in turn, is connected to the central office TC (Figure 1). The radio beacon 2 makes it possible to generate, for example, DSRC-based toll transactions based on its radio communication 5 with vehicle devices (Onboard Units, OBUs) 6 that are carried along by vehicles 7 passing the station TE on a road 8.

The camera 3 makes it possible to generate video-based control transactions in that the camera 3 records an image pic of the vehicle 7, in which the vehicle identification 9 on a license plate of the vehicle 7 is subsequently read by means of optical character recognition (Optical Character Recognition, OCR). The result of the OCR evaluation of the recorded image pic in the form of the vehicle identification 9 forms the basis of a video-based control transaction tr - for example, after it was

supplemented with a current time stamp, a measured speed value of the vehicle and/or an identification of the control station TE or camera 3 - and is sent to the transaction receiver CI via a central office TC.

The vehicle identification 9 that can be read by means of OCR may consist of the registered license number of the vehicle or of another identification of the vehicle that can be read by means of OCR such as, e.g., a hazardous materials identification, a fleet identification, etc.

In order to enable the transaction receivers CI to carry out a validation (authentication) of such video-based transactions tr, video-based control stations TE are equipped with a separate processing element (Authentication Entity) AE that may be assigned to the entire control station or individually to one or each camera 3 thereof.

In a first step 11, a cryptographic key (trusted key) tk specifically assigned to and trusted by a transaction receiver CI is stored in the transaction receiver CI, as well as in each control station TE, from which control transactions tr should be received, particularly in the respective processing element AE of the control station TE (Figure 1).

Figure 3 subsequently shows the signal flows or processing steps being carried out when a vehicle 7 passes a control station TE that is equipped with such a processing element AE and generates a control transaction tr that is sent to an exemplary transaction receiver CI via the operator's central office TC. The cryptographic keys tk of the different transaction receivers CI, to which the control station TE can send control transactions tr, were already stored in the processing element AE; see tk-dataset 12.

The camera 3 records an image pic of the vehicle 7 while it passes the control station TE and a control transaction tr is generated from the recorded image in an OCR process 13 based on the result of reading the vehicle identification 9 by means of OCR. The control transaction tr may contain other data such as a time stamp, an identification of the control station TE and/or camera 3, an identification of the processing element AE, a serially incremented count value (transaction counter), etc. It goes without saying that the OCR process 13 could also be calculated in a geographically remote (not-shown) proxy computer to be assigned to the control station.

The processing element AE receives the recorded image pic and generates a random key rd therefor. Based on this random key rd, a random image section p is extracted from the recorded image pic and a hash value h(p) of the image section p is formed, e.g., by means of a modulo addition of the image pixels in the image section p, namely in a process 14. For this purpose, the random key rd directly specifies, for

example, the image coordinates of at least three image pixels in the recorded image pic that generate or define the image section p. Alternatively, the random key rd could also specify certain properties of image pixels such as, e.g., color values, wherein all image pixels with these properties then form the image section p.

The extraction of a random image section p from the recorded image pic and the formation of a hash value h of the image section p only requires minimal computing power and therefore can also be realized in real time, e.g., with a simple processor means in the processing element AE such as, for example, a processor means of the type provided on chip cards or SIM card processors.

In a process 15, the thusly formed hash value h is subsequently encrypted again with the cryptographic key tk of the respective transaction receiver TE [sic], to which the control transaction tr is sent. However, the encryption process 15 may also be realized by once again forming a hash value of the aforementioned hash value h and the cryptographic key tk.

The correct key tk can be selected, for example, based on allocation lists ("white lists") of vehicle identifications 9 and appropriate transaction receivers CI, i.e., the result of the OCR process 13 controls the selection of the cryptographic key tk from the set 12 (arrow 16).

The resulting authentication data au obtained at the output or end of the processor 15 is added to the control transaction tr together with the random key rd such that it is expanded into a supplemented control transaction {tr, rd, au} 17. In this case, other data such as a time stamp, an identification of the control station TE and/or camera 3, an identification of the processing element AE, a serially incremented count value (transaction counter), etc., may also be added to the authentication data au or integrated therein.

The supplemented control transaction 17 is subsequently sent to the transaction receiver CI via a first transmission channel 18 that, e.g., also comprises an operator's central office TC along its path. The basis of the control transaction tr in the form of the recorded image pic is also sent to the transaction receiver CI via a second transmission channel 19. The transmission via the first and the second transmission channel 18, 19 does not have to take place simultaneously; for example, the supplemented control transactions 17 and - preferably - the recorded images pic can also be intermediately stored, e.g., in databases 20 of the operator's central office TC and retrieved by the transaction receiver CI, wherein this procedure also falls within the scope of the term "sending" in this context. Another option consists of adding the authentication data au

and the random key rd to the image data pic rather than the control transaction tr. All data tr, rd, au, pic can also be sent via the same transmission channel.

It goes without saying that only a single encryption process or encryption step may also be carried out in the processing element AE in simplified embodiments instead of the preferred processes 14, 15 shown, wherein the recorded image pic is encrypted into the authentication data au with the random key rd and the cryptographic key tk in one step during this single encryption process. For example, the random key rd and the cryptographic key tk could be combined into a common key that is applied to the recorded image pic in order to obtain the authentication data au.

The received supplemented control transactions 17 and the recorded images pic forming the basis thereof are subsequently combined , i.e., assigned to one another, in the transaction receiver CI, for example, based on at least one mutual reference in one of these datasets such as a reference to a specific identification of a recorded image pic in the control transaction tr or a reference to a specific identification of a control transaction tr in a recorded image pic or both. The transaction receiver CI could also merely validate control transactions tr at random in that it only processes or receives the correspondingly assigned recorded image pic, e.g., from the database 20 of the operator's central office TC upon a corresponding request, in case there is a reason. An assignment is not necessary if the recorded image pic is received together with the supplemented control transaction 17.

In a first step 21, the random key rd is now extracted from the supplemented control transaction 17 in the transaction receiver CI and applied to the received and assigned recorded image pic in a process 22 identical to the process 14 in the processing element AE in order to once again obtain the random image section p and to form the hash value h thereof. The latter is once again encrypted with the cryptographic key tk of the transaction receiver CI in a process 23 that is identical to the process 15 carried out in the processing element AE in order to obtain reference or nominal authentication data au_r. This data is subsequently compared with the authentication data au extracted from the supplemented control transaction 17 in a step or process 24 and the transaction tr is validated if the two authentication datasets are identical, i.e., the transaction is considered to be authenticated and cleared for further processing and/or billing in the transaction receiver CI. If the two authentication datasets are not identical, an error or a manipulation has occurred and the transaction tr is not validated (invalid) and discarded; a corresponding alarm message can be output and logged in this case.

It is optionally also possible (although not shown) to store several different cryptographic keys tk_i for each transaction receiver CI in the dataset 12 of the

processing element AE and in the transaction receiver CI - together with a respectively assigned key identification tkID. A key tk_i of the respective transaction receiver CI is then selected in the processing element AE together with its key identification tkID and used for the encryption. The key identification tkID of the key tk_i used is then added to the authentication data au and used for identifying the correct key tk_i in the transaction receiver CI.

The processing element AE may be realized in the form of a cryptographically secured software module or - preferably - in the form of a physically secured hardware element. The processing element AE can be connected, in particular, to the control station TE - that also may simply consist of the camera 3 only - via a physical interface 25. It is ensured that an unauthorized separation of the interface 25 renders the processing element AE in the form of a hardware element unusable, e.g., in that a separation of the interface 25 irretrievably erases the memory of the processing element AE or at least permanently blocks any access to the cryptographic keys rd, tk stored therein.

The invention is not limited to the illustrated embodiments, but rather also includes all variations and modifications within the scope of the attached claims.

2012200542 02 Oct 2013

Claims

1. A method for validating a road traffic control transaction that is sent from a control station of a road traffic control system to a transaction receiver of the road traffic control system in the transaction receiver, including the following steps:

storing a cryptographic key assigned to the transaction receiver in the transaction receiver and in a separate processing element of the control station;

recording an image of a vehicle, reading an identification of the vehicle in the recorded image by means of OCR and generating a control transaction thereof in the control station;

generating a random key which defines an image section in the recorded image and encrypting the recorded image into authentication data with the random key and the cryptographic key in the separate processing element by the processes

-extracting the image section from the recorded image;

-forming a first hash value of the image section; and

-encrypting the first hash value with the cryptographic key into the authentication data;

sending the recorded image, the control transaction, the random key and the authentication data to the transaction receiver;

in the transaction receiver: encrypting the received recorded image into nominal authentication data with the received random key and the stored cryptographic key by the same process as conducted in the processing element; and

comparing the received authentication data with the nominal authentication data,

wherein the received control transaction is validated if the two datasets are identical.

2. The method according to Claim 1, wherein the aforementioned encryption of the recorded image with the cryptographic key comprises the step of forming a second hash value of the first hash value and the cryptographic key, wherein the second hash value represents the authentication data.

3. The method according to Claim 1 or 2, wherein several cryptographic keys assigned to different transaction receivers are stored in the processing element and the cryptographic key to be respectively used is selected depending on the identification read by means of OCR.

4. The method according to any one of Claims 1 to 3, wherein the authentication data and the random key are sent to the transaction receiver together with the control transaction.

5. The method according to any one of Claims 1 to 3, wherein the authentication data and the random key are sent to the transaction receiver together with the recorded image.

6. The method according to any one of Claims 1 to 5, wherein a time stamp, an identification of the control station, an identification of the processing element and/or a serial count value is integrated into the authentication data.

7. The method according to any one of Claims 1 to 6, wherein several cryptographic keys are stored in the transaction receiver and in the processing element together with assigned key identifications, wherein the key identification of the key used is integrated into the authentication data and used for determining the assigned key in the transaction receiver.

8. The method according to any one of Claims 1 to 7, wherein a hardware element is used as the aforementioned processing element and connected to the control station via a physical interface.

9. The method according to Claim 8, wherein a separation of the interface renders the hardware element unusable.

10. A method for validating a road traffic control transaction substantially as hereinbefore described with reference to the accompanying drawings.

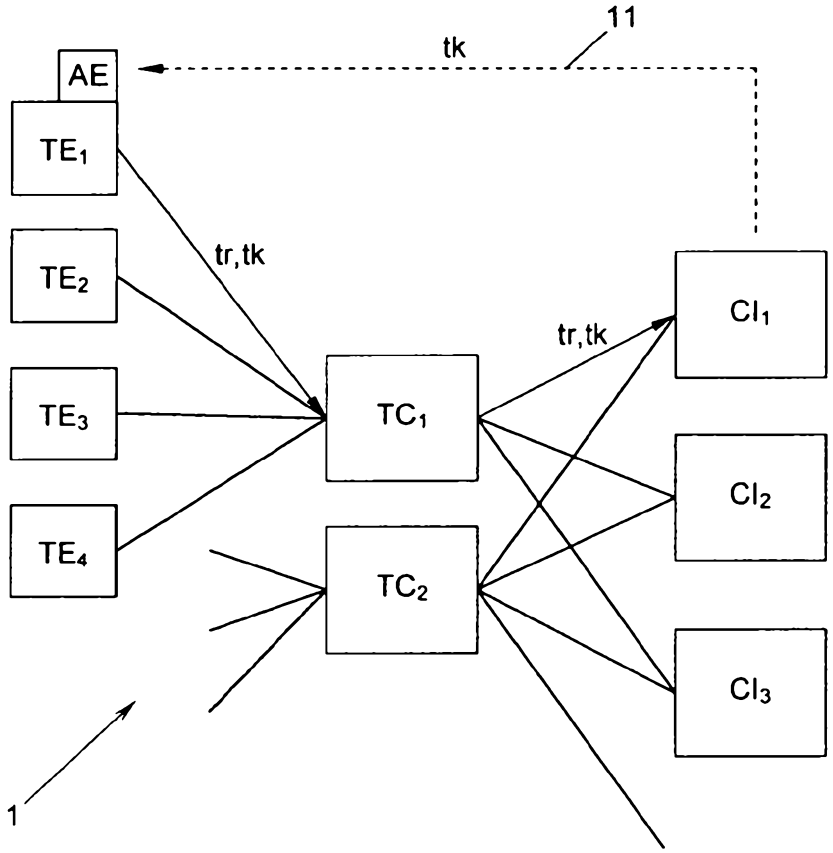
11
tk
AE
TE1
TE2
TE3
TE4
tr,tk
TC1
TC2
tr,tk
CI1
CI2
CI3
1

Fig. 1

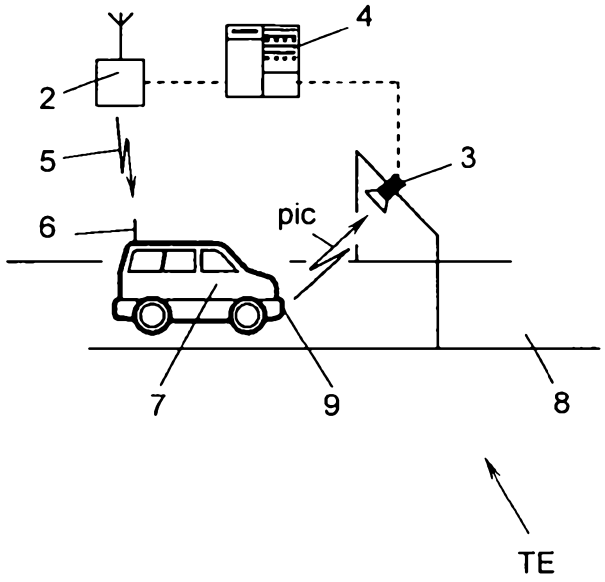
4
2
5
3
6
pic
7
9
8
TE

Fig. 2

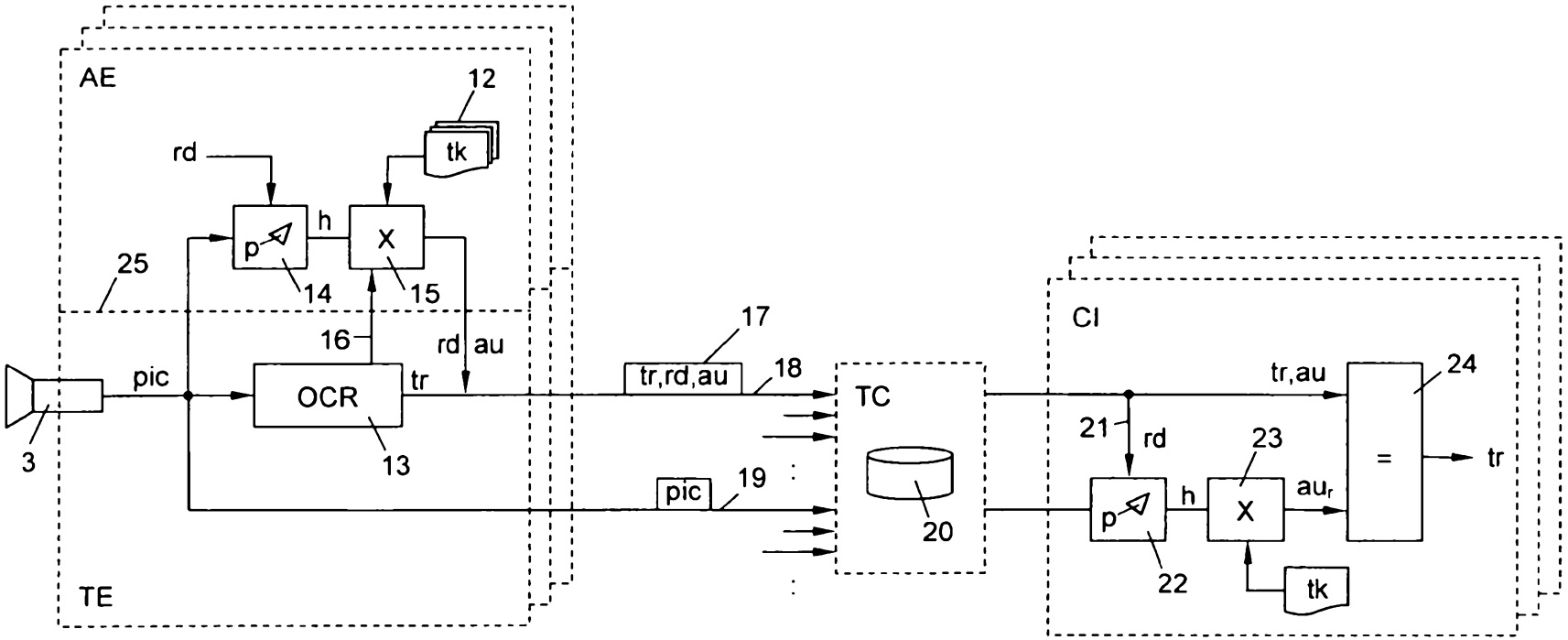
AE
12
tk
rd
h
p
X
14
15
25
16
rd
au
17
pic
OCR
tr
tr,rd,au
18
TC
3
13
pic
19
20
CI
tr,au
24
21
rd
23
=
tr
p
h
X
au_r
22
tk
TE

Fig. 3