166166

- 8 SEP 2003

The Traffic Information & Pricing (TIP) system

1 Introduction

In this introduction we first describe our use of the notion of traffic information system, show what such a traffic information system can be used for and give a few properties that a traffic information system preferably must have. Then we give a short description of a few characteristic aspects of traffic information systems associated with the invention, i.e. of TIP systems. Then we focus on a specific, important application, namely traffic pricing, before giving a further characterization of TIP systems used – exclusively or also – for traffic pricing. After a comparison with existing systems, we give a closing overview of the further content of the text, where further explanation will be given.

1.1 Traffic and infrastructure

Traffic makes use of – at least a part of – an *infrastructure*, that is, the collection of all provisions for traffic, such as a traffic network consisting of traffic ways and all kinds of associated objects. For example, the infrastructure in the case of shipping traffic consists of, among others, waterways, harbors, radar stations, beacons, navigation or satellite navigation systems and shipping communications systems, such as maritime phones. With this example, we hope to have illustrated that the notion infrastructure must be interpreted in a broad sense.

With the notion *traffic* is not only aimed at 'physical' traffic (such as transport over, under and/or via land, water and air), but also at 'logical' traffic (such as, for example, message traffic in computer networks and/or economic traffic). Even though TIP systems can be used, possibly in adjusted form, by such other forms of traffic[1], we restrict ourselves in the following explanation to 'physical' traffic. In order not to unnecessarily complicate the description of TIP systems and of the required and/or applied techniques, we concentrate ourselves in the following examples and the further explanations mostly on the instance of road traffic. Based on the given explanation, a person skilled in the art can create by himself/herself a description, modified where necessary, for other forms of traffic or transport. The examples given and the variations mentioned are intended for illustration only and thus must not be interpreted as imposed restrictions.

1.2 Traffic information and traffic fee

The term *traffic information* will be used for every relevant bit of information related to traffic in the broadest sense, including also information on the infrastructure involved, the relevant persons and/or vehicles (for example, taking part or having taken part in traffic), the use of vehicles, and other relevant aspects, such as, for example, traffic congestion, weather conditions or other usage conditions[2].

We use the term *traffic fee* [alternative translation: traffic levy] not only for traffic taxes, such as, for example, road taxes and tolls, but also for all kinds of other costs that one way or another are related to participation in traffic, such as, for example, traffic fines, transport costs and insurance premiums. For transport costs, think, for

---

[1] Think, for example, of charging for data transport or perhaps even on electronic charging of sales tax, salary tax and/or income tax.

[2] For example, in case of shipping traffic tide tables could be relevant information. See also the next footnote.

G00002

8 SEP 2003

example, of the costs for the use of public transportation, and for insurance premiums, think, for example, of the fees for car insurance, where the amount, for example, could depend on the number of driven kilometers and/or on the location where the kilometers were driven. (For example, because the risk of damage per driven kilometer on a freeway is lower than on a secondary road or in a city center.) Further, we interpret traffic fees to include not only fees for active traffic participation, such as, for example, in the case of road traffic pricing, but also for passive 'participation', such as, for example, in case of parking fees. In summary, our term traffic fee has, just as our term traffic information, a – very – broad interpretation.

1.3 Traffic information system

When collecting and/or disseminating traffic information one speaks of, what we will call, a *traffic information system*. A traffic information system can, for example, be used for *collecting* information on the traffic intensity or the utilization degree of – at least a part of – the road network, about traffic congestion delays, about fuel consumption, about amounts of environmental pollution caused and/or related to payable traffic fees. A traffic information system might be used (exclusively or also) for the *dissemination* of information on, for example, distances, speed limits, traffic delays, outside temperatures, air pollution[3] and/or reduced visibility (e.g. fog banks).

A traffic information system *can* be used for diverse goals, such as for:

- The supporting of traffic management and control, in the broadest sense;
  think, for example, of traffic control, traffic census, the tracking of traffic flows and the measuring of their average speed, the determination of the distance between successive vehicles, the detection of tailbacks and the measuring of traffic delays, but also on determining and/or planning of the need for expansion of the infrastructure, because management (in the broadest sense) of the infrastructure also falls within this scope.
- The improvement of traffic safety;
  for example, through continuous and – more – efficient speed checks, through immediate warnings for fog banks and/or through cruise controls with automatic respect for local speed limits, spread via transmitters.
- The collecting of information on fuel consumption of vehicles in practice;
  the results could for example be divided into make, model, year, gearbox type, engine type, speed, acceleration, gear engaged, engine speed, engine temperature, weather conditions, etc.
- Determining as accurately as possible the environmental pollution caused by the traffic or by a part of the traffic;
  for example as an aid in the making of, or compliance with, agreements on reductions in environmental pollution.
- The calculation, and possibly also the charging, of traffic fees;
  price calculations only, such as could be the case for travel by taxi or for insurance premiums, or also the actual charging, such as could be the case for public transportation or traffic pricing; an important aspect in all this is the ability to introduce or improve *proportionate pricing*.

---

[3] Think of – timely – warning for extreme air pollution in, for example, tunnels. Air pollution is an example of usage conditions.

-8 SEP 2003

- For improvement of law enforcement;
  for example, through automated detection of all kinds of traffic offenses, through automated and reliable identification, through association of traffic offenses with individual persons for use in a penalty points system, through better automation and greater reliability of the settling of traffic fines and/or through quick and simple tracking to combat vehicle theft.
- For support in managing, in a broad sense, a vehicle fleet[4];
  for example, the vehicle fleet of a taxi, car rental or transport company.

1.4 The TIP system

The TIP system[5] is a traffic information system that can be used for all of the aforementioned goals, for each goal apart as well as for many or possibly even all goals simultaneously[6]. Due to its broad applicability, the TIP system can be rightly called a *multifunctional traffic information system.* Because in the TIP system – all or a part of – the applications might also be compiled into one integrated, larger whole, one can also speak of an integrated multifunctional traffic information system.

1.5 The authority

Due to the many and diverse tasks that a TIP system can perform, it is very well thinkable that multiple authorities [alternative translations: official bodies, corporations, organizations] are involved in the diverse applications of a TIP system. In such a case, the TIP system will most likely be managed or controlled by one or more of the authorities involved or by a separate authority, not directly involved in one of the specific applications. The manager or controller is (or, the joint managers or controllers are) responsible for the TIP system and for the services to the rest of the authorities involved. Here again, management or control should be taken in a broad sense and thus encompasses, among other things, maintenance, protection, adaptation, expansion, keeping operational, etc.

To prevent our explanation from becoming unduly complicated, when referring to one or more of the above-mentioned authorities (including the manager or controller), we will often use the term *the authority* (or: an authority) below. The singular term authority can therefore be used to reference a certain separate authority, which is responsible for or has interest in a specific application, but also for all (or a part of) the involved authorities together. Sometimes we also use the description 'information collecting and/or verifying authority'.

1.6 A number of desired properties

A traffic information system must preferably have at least the following properties:

- Being automated as much as possible;
  this is of importance, for example, with respect to celerity and usage costs; fast collection and dissemination of recent information is of importance, as is avoiding staffing costs as much as possible.
- Functioning without disturbing traffic;

---

[4] This example might be placed – at least for a part – within the broad notion of traffic control.

[5] We usually say 'the system', although actually it concerns a class of many systems with certain characteristics.

[6] For clarity, we emphasize that one can also – wish to – collect information about speeds and/or environmental pollution caused by traffic without using this information for law enforcement and/or traffic fees.

-8 SEP 2003

this is relatively easy to achieve, for example through the use of transmitters and receivers.

- Being prepared for 'growth';
  to protect the investment, the system should be adaptable and extendible (i.e. flexible), so that for example new applications can later be added relatively easily. (See also Chapter 17.)
- Providing for sufficient privacy protection;
  this particularly concerns privacy protection with respect to movement patterns, or hindering (i.e. not making practically feasible or easier) illegitimate *tracing* of individual, uniquely identifiable persons and/or vehicles[7].
- Guaranteeing sufficient reliability of the collected information;
  this concerns, for example, sufficient *fraud resistance*, which is particularly of importance if the collected information is used to calculate and/or charge traffic fees.

In general, the first two mentioned properties, at least for a large part, can be achieved in a rather obvious manner, namely by using computers, transmitters and receivers. Realization of the last two properties is much harder, certainly in combination. After all, exercising a certain amount of supervision is indispensable for, among other things, reaching – at least a part of – the desired fraud resistance. And for checking[8] it is generally necessary to identify the checked object. Thus, checking and identification generally go hand in hand. Unique identification of persons and/or vehicles during the collecting and/or checking of information, however, forms a privacy threat, because this often enables or facilitates tracing of the persons and/or vehicles in question. Through this coarse reasoning, we hope to have given sufficient explanation as to why checking generally becomes more difficult if at the same time privacy has to be protected (and vice versa).

1.7 Global characterization of TIP systems

Based on the above-mentioned elucidation, we can state that traffic information systems will differ from each other in particular with respect to the methods used to provide for adequate checking and/or privacy protection[9]. It should be no surprise that the TIP system distinguishes itself from other traffic information systems mainly by these two aspects and the possibilities of combining them. For clarity, we emphasize that the TIP system gives the option of combining all of the mentioned properties. We are now ready for a first, concise characterization of the TIP system.

The class of traffic information systems associated with the present invention, i.e. the TIP system, is especially characterized by the way in which the following properties are provided:

---

[7] 'Privacy protection with respect to movement patterns' and 'hindering illegitimate tracing' mean the same to us. The addition of 'with respect to movement patterns' will often be left out and the addition 'illegitimate' will sometimes be left out. We also speak often of 'prevention' instead of 'hindering' or 'not making practically feasible.' (See also the elucidation to Claim 1 elsewhere in this chapter.) What exactly is meant will generally become apparent from the context.

[8] Checking [alternative translation: verification] and supervision are, or at least are used by us as, synonyms. Thus, checking also comprises supervising.

[9] Here privacy protection of course refers to the prevention, i.e. the hindering, of tracing.

- The property that certain information on persons and/or vehicles, in particular also on *individual* persons and/or vehicles, can be collected and – as far as necessary – can be *checked* on reliability by (or for) the authority;
- The property that in that event the authority does not have to rely on the *fraud resistance* of components in vehicles other than agents possibly present in vehicles (see below);
- The property that in that event illegitimate *tracing* of individual, uniquely identifiable persons or vehicles can be prevented.

1.8 Tracing

It should be clear by now that the last-mentioned characteristic means that the information collecting and/or verifying authority generally does not need to obtain access, or reasonably cannot even obtain access, to information (considered to be privacy-sensitive) about the movement pattern of a certain vehicle or a certain person of which the identity, or whose identity respectively, can be retrieved. More elucidation will be given in Chapter 3.

1.9 Fraud resistance and checks

In a strict sense, one can only speak of fraud resistance if there are no possible means of fraud. In practice, one usually speaks of *fraud resistance* as soon as there is resistance to all known, practically achievable, profitable forms of fraud that one wishes to be protected against. We use the term *fraud-resistant* particularly in the latter sense. We will discuss this term and its uses somewhat deeper in Chapter 4. There, we will also give a further explanation to the meaning of the terms fraud-resistant and fraud resistance when applied to an individual component.

Fraud by providing incorrect information in or from a vehicle is hindered by *checking* the received information. Checks can therefore provide for at least a part of the fraud resistance. However, information can be incorrect not only due to fraud (or fraud attempts), but also in good faith due to, for example, inaccuracy or malfunctioning of certain equipment. Thus, checks on the reliability of information are useful for more than fraud deterrence [alternative translation: fraud combating] alone. Since both terms are closely related, they sometimes will be used in this text more or less as a kind of synonym.

1.10 Agent

The term *agent* will be used for every hardware and/or software component that:

- now and then actively performs in a vehicle one or more tasks for the authority, and
- must be fraud-resistant (as seen from the viewpoint of the authority).

At the risk of laboring the obvious, we mention that the last point implies already that the correct performance of the task mentioned in the first point is essential to the protection of the interests of the authority and therefore to the correct working of the traffic information system. In other words, an agent serves the interests of (or represents) the involved authority in the vehicle and is a component of which the proper, i.e. not manipulated, functioning can and must be trusted by the authority, in particular also in an environment as formed by a vehicle that – from the standpoint of fraud prevention – can be considered to be an insecure environment.

What an agent exactly is, or can be, will undoubtedly become clearer when reading the complete text. For tasks to be performed by an agent think, at least tentatively, of – partly or fully – checking the reliability of certain

= 8 SEP 2003

information supplied by other components in the vehicle. In Chapter 18, the reader will find an extensive enumeration of tasks that can be performed by an agent.

1.11 Characterization of the methods for the hindering of tracing

The methods by which a TIP system can provide for privacy protection with regards to movement patterns is characterized in particular by the use of at least one of the following three elements:

- *Semi-identifications*;
  Semi-identifications can, as we will demonstrate later, be used for privacy-friendly collecting of certain information, such as, for example, for fully automated and precise, up-to-the-minute determination of the current traffic delays. More in general, the use of non-unique semi-identifications helps to reduce the use of privacy threatening, unique identifications of vehicles and/or persons.
- *Agents*;
  Agents can, as we will demonstrate later, be used for the collecting and checking of all kinds of information in such a way that there is no or hardly any need for the use of privacy threatening, unique identifications of vehicles and/or persons.
- *Hunters and/or intermediaries*;
  Hunters and/or intermediaries can, as we will demonstrate later, be used for collecting, somewhere outside of a vehicle (i.e. in the outside world), information that has been transmitted from the vehicle and that does contain data uniquely identifying the person and/or vehicle in question, in such a way that sufficient protection against illegitimate tracing is provided for.

1.12 Characterization of the method for performing checks

The manner in which, in a TIP system, an authority can verify the reliability of, and thus can hinder fraud with, certain information supplied to it in or from a vehicle, including particularly also various kinds of *counter values*, has two manifestations:

- Only checking by the authority *from a distance*;
  the interests of the authority then are sufficiently protected without any of the involved individual components in the vehicle (transmitter, receiver, sensors, meters, counters, connections, and the like) having to be fraud-resistant.
- All or some of the checks by the authority are performed with the help of *agents in the vehicles*;
  the interests of the authority then are sufficiently protected without any of the *other* involved individual components in the vehicle (transmitter, receiver, sensors, meters, counters, connections, and the like) having to be fraud-resistant.

As we do wish not to interfere with traffic unnecessarily, it seems plausible to carry out – at least a part of – the necessary inspections from a distance, that is, to perform from outside of the involved vehicle – all or a part of – the checking on the reliability of the information transmitted by that vehicle. The use of certain identifications seems difficult to avoid, at least during – remote – checks.

-8 SEP 2003

It will appear that the approach using agents offers more, or better, possibilities than the approach using remote checking exclusively[10]. Yet one can achieve surprisingly much with exclusive remote checks. Later chapters will give more details.

1.13 Charging traffic fees with the aid of a traffic information system

As mentioned earlier, it is possible to use a traffic information system – also or exclusively – for levying traffic fees, also including at least tolls, traffic fines, road taxes, insurance premiums and parking fees. Because this is a very important application, we will now explore this possibility further. In this section, the emphasis of our further elucidation lies on traffic pricing. Also, in the further treatment and explanation in the coming chapters, this application will often be the central theme. The fact that we focus our attention primarily on traffic pricing has not only to do with its importance, but particularly also with the fact that this application is well-suited to illustrate and explain a considerable portion of the possibilities that the TIP system offers.

Traffic pricing may be used merely as a form of taxation, but for example also as an *environmental* protection *measure* and/or as a *measure* to improve the *reachability* [alternative translation: accessibility] of certain areas at certain times. When using it as an environmental measure, one wants, also in areas free from tailbacks, to prevent the unrestricted growth of the amount of traffic or perhaps even to reduce the amount of traffic, since traffic participation always goes hand in hand with energy consumption and with a certain degree of environmental pollution.

Although from a qualitative perspective this last statement is absolutely correct, one should not forget that, quantitatively seen, there can be large differences in the degree of environmental pollution caused. Think, for example, of the differences between the various kinds of transport (for example cars vs. busses, but more in general, for example, air transport vs. maritime transport or train traffic vs. road traffic), between the various kinds of propulsion engines (for example, electric engines vs. combustion engines, but also the one type of gasoline engine vs. another type) and between the various kinds of fuel used (for example, solar energy vs. fossil fuels or Liquefied Petrol Gas vs. gasoline).

When imposing traffic fees it may, for example for the sake of justice, be a desired situation that *all* kilometers (or whatever distance units) are taxed and that kilometers traveled under the same relevant conditions (say, with exactly the same kind of vehicle, same speed, same kind of fuel, etc.), are taxed equally. Just suppose that in a certain country traffic pricing is introduced solely as an environmental measure. Then it would seem reasonable, for example, that kilometers traveled in an urban environment in that country are taxed just as heavily as kilometers traveled in a rural environment, at least if they are traveled under the same relevant circumstances [alternative translation: conditions] (thus, in this case: with the same environmental consequences). After all, for the environment in a certain region it generally makes little difference whether the polluting exhaust gases are produced in a rural or in an urban environment within that region.

But it may also be desired to indeed make the tariff, even in case of equal pollution, vary for each kilometer traveled, for example depending on the traffic intensity or on time and location. This kind of tariff settings can be

---

[10] This last approach we sometimes refer to – sloppily – as the approach without agents, even though strictly speaking this certainly is not the same.

-8 SEP 2003

used, for example, to improve the reachability of certain areas at certain times, e.g. by combating tailbacks during rush hours.

In this text, we prefer to refrain from a discussion about – the justice of – all kinds of reasons for imposing, or wanting to impose, traffic fees. We do remark, however, that it is beneficial for the general suitability of a traffic information system for imposing all sorts of traffic fees, if the tariff settings can be varied in such a way that all kinds of possible wishes, among which the two mentioned above, can be met.

Therefore, it must preferably be *possible* to make the tariff for a traveled distance unit dependent on (or it must be *possible* to ascertain *reliable* values of) as many variables as possible, such as, for example, the date and time when (more precisely formulated: the exact period in which), the location where and/or the traffic congestion when said distance unit was traveled, all or a part of the complete *classification* [alternative translations: characterization, typing], (i.e. the brand, model, year of make, gearbox type, engine type, and the like) of the vehicle used, the kind of fuel, the fuel consumption, the gear engaged, the amount of noise produced, the kind and amount of the environmental pollution caused, the average speed, the engine speed, the [vehicle] speed change or changes and/or the engine speed change or changes with which said distance unit has been traveled with said vehicle.

1.14 Possible use of derived information

Between certain variables there exists a certain connection. For example, there exists for every vehicle of a certain year of make, type and model that is equipped with a certain gearbox type and engine type, a connection between the fuel consumption at a certain moment and a few other quantities at that same moment, such as, for example, the outside temperature, the speed, the engine speed and the acceleration. Something similar is valid for the amount of noise produced and for the amount of pollution caused. If such a connection is, also quantitatively, sufficiently accurately known, it can be used for sufficiently accurate determination of derived values, i.e. for sufficiently accurate calculation or deduction of certain quantities from other ones.

Sufficiently accurately derived values can be used in two ways, namely for checking, i.e. comparison with a value that – as reported – is actually measured, or for leaving certain measurements undone. The first-mentioned possibility is the case, for example, when the reliability of reported fuel consumption is being checked. The second-mentioned possibility is the case, for example, if one determines the kind and amount of the air pollution caused at a certain moment by a certain motor vehicle without at that moment actually measuring and analyzing by the vehicle concerned the kind and amount of its exhaust-fumes[11].

1.15 A characterization of the TIP system when used for traffic pricing

An important characteristic of TIP systems intended, or also intended, for traffic pricing is that all earlier mentioned wishes can be met. Characteristic for the checking methods used for such TIP systems is that particularly

---

[11] Although we assume that the actual measurement and analysis of the exhaust gases of each vehicle is too expensive, it can in principle be done. However, the actual measurement from a motor vehicle in traffic of the total amount of noise that is produced by this same vehicle (thus including the noise from air rushing along the vehicle), seems impossible, also because of the possible presence of much other traffic in the vicinity. Rather accurate derivation of the total noise production of a vehicle from other data therefore seems to be even mandatory.

-8 SEP 2003

also fraud with regard to certain counter values can be combated, so that the said traffic information systems can also collect reliable information on counter values. This has as a consequence that the collected information also can be used for a fraud-resistant implementation of *continuous pricing* [alternative translation: imposing a continuous fee]. (In Chapter 2 we will come back to this notion, which concerns a levy whereby the total 'consumption' expressed in, for example, kilometers or, for example, in a certain environmental pollution unit can be charged.) Thus, the desire to be able to charge for *all* traveled kilometers (hectometers, miles, or whichever distance units) can also met, among other things.

Briefly summarized, the TIP system thus encompasses, among other things, a class of systems for computing and possibly also charging traffic fees in which *all* traveled distances can be charged, the tariff per traveled distance unit (for example, per kilometer) being variable in many ways, in which also extra costs for the use of certain sections of roads (toll roads, bridges, tunnels, and the like) can be charged, in which sufficient privacy protection and fraud resistance can be offered and in which (as we will show later) extensions, refinements or possible other changes can be easily be introduced later on. The tariff for a traveled distance unit can, in case of the TIP system, be made dependent on all kinds of variables, such as, for example, the traffic intensity, the type of the vehicle (i.e. brand, model, year of make, gearbox type, engine type, and the like), the sort of fuel, the fuel consumption, the gear engaged, the noise, the average speed, the engine speed, the [vehicle] speed changes and/or the engine speed changes with which the distance unit has been traveled, and/or the date and time when (more accurately formulated: the precise period in which) this distance unit has been traveled. A notable aspect thus is that it is possible to charge for all kinds of environmental pollution (such as, for example, noise and air pollution) caused by the use of a certain vehicle, without actually having to analyze and measure by the vehicle in question continually the kind and volume of that pollution. For clarity, we here already emphasize that our system is not only suitable for continuous pricing, but also for other kinds of levies, such as open and closed tolling (see Chapter 2).

1.16 The need for the TIP system for traffic pricing

In certain countries, taxes are currently already levied in various ways on traffic in a wide sense. Think, for example, of taxes on the purchase, ownership and the use of vehicles. In case of these existing forms of traffic fees, one can not, or insufficiently, take into account, for example, the amount, the locations and the times of the use of a vehicle and the amount of the resulting environmental pollution.

For example, in case of the levying of excise on fuel, which can be considered to belong to the third above-mentioned category of taxation, the amount of use really does play a role. But yet also this form of traffic pricing is clearly lacking. For, one cannot take into account, for example, the location and/or the time of use, nor the fact that a certain amount of fuel can be consumed in a more or in a less environmentally friendly way. Furthermore, there is the practical problem that the excises on fuels usually cannot be raised or lowered at will without creating serious problems. Think, for example, of the consequences for gas station owners in borderlands and of the possible loss of tax revenues due to legal and/or illegal import of fuel from a neighboring country. In short, the ex-

8 SEP 2003

isting forms of traffic pricing can, as yet, insufficiently meet the wish for more or better *proportioning* [alternative translation: 'variabilization'][12].

There is thus really a need for a practically usable, effective and flexible system for the levying and/or proportioning of all kinds of traffic fees, such as, for example, fees for the use of a vehicle (taking into account the amount, the locations and/or the points of time of use and/or the amount of pollution caused) and for the use of certain sections of road (toll roads, toll bridges, toll tunnels, and the like), without having to violate the privacy of users or payers. The TIP system is such a system. Besides, the TIP system can also fulfil, among other things, the desire to be able to determine in real-time traffic delays expressed in minutes (or in some other time unit) in a cheap and privacy-friendly way.

1.17 Comparison with existing systems for traffic pricing

For traffic pricing, many systems have already been contrived. Often this concerns toll systems whereby toll is charged only when passing certain toll points. Such toll systems thus only support the kind of levy that we will call *open tolling* (see Chapter 2). Open tolling forms a rather coarse and narrowly usable means that in many cases will be lacking. It can be used for improving the reachability, but is not suitable for use as an environmental protection measure[13]. Furthermore, it is a disadvantage that use of open tolling often leads to all kinds of unfair situations.

Suppose, for example, that around a certain area a completely closed cordon of toll points is introduced as a measure to improve the reachability, i.e. in order to levy toll during rush hours (and thereby to discourage the access to that area with a motor vehicle) with the intention to relieve the road network within that area to a certain extent. In the situation sketched, some may continually criss-cross this area during the rush hours and thus continually burden the road network in question after having paid toll only once (during rush hours to gain access to the area) or not even once (if they are already within the area before the rush hours begin). However, others do have to pay toll (or must pay the same amount of toll) for making only one short trip during rush hours. Or they may even have to pay toll several times for several short trips.

We know of no system that, just as the TIP system, is fraud-resistant and also can apply per person and/or per vehicle *many* forms of *continuous pricing,* such as, for example, in relation to the – total – fuel consumption, the – total – noise production and/or the – totally – caused environmental pollution. At the least we know of no single existing system whereby the noise and/or the emission or, more general, the environmental pollution caused by individual vehicles is computed rather accurately, let alone a system whereby such calculations play a role in charging traffic fees. Also we do not know of any system that can verify whether the fuel consumption reported in or from a vehicle is correct, i.e. reliable. In short, as far as we know the TIP system is unique with respect to the

---

[12] If, for example, the type of a vehicle is used as a variable, one can relate the tariffs to the environmentally friendliness (or unfriendliness) of vehicles of that type. And so one can, via the tariffs, stimulate the purchasing of the most environmentally friendly vehicles in a much better addressed way.

[13] We will not elaborate here on the arguments that this assertion is based on. We only note that open tolling can in principle even have a negative effect on the environment, because traffic will try to avoid toll points as much as possible.

number of aspects about which reliable information can be collected. (Think, for example, also of traffic intensity.) As a consequence, the TIP system is also unique with respect to the extent to which various forms of continuous pricing can be applied.

There do exist a small number of systems that, just as the TIP system, can be used for the application of the *one* specific form of continuous pricing whereby all traveled kilometers are charged. However, to the best of our knowledge it is true for all these systems at least that they either offer insufficient protection against tracing; or that they use a – relatively expensive – Global Positioning System (GPS), or that they are either insufficiently or less fraud-resistant, or that they have to make – more – extensive use of physical protection measures in order to reach a sufficient level of fraud resistance.

1.18 Some unique aspects of the TIP system

A unique aspect of the TIP system is, therefore, that all kinds of continuous pricing can be realized and that effective measures can be taken against fraud and against tracing of individual, uniquely identifiable persons and/or vehicles without the necessity of physically protecting the involved components in vehicles, other than possibly present agents, against fraud and without having to use GPS.[14]

Besides, the TIP system has much more to offer. For example, the possibility to collect fully automatically and in a very privacy-friendly manner the most recent information on traffic delays, which expressed in minutes are much more informative than information on tailbacks expressed as lengths in kilometers. Further we mention here the possibility of identifying vehicles in a privacy-safe and/or fraud-resistant manner and to acquire better insight in the actual traffic flows, the possibility of systematically collecting reliable data from practice, for example, about the fuel consumption realized in practice per vehicle type, and the possibility of effectively combating theft of vehicles.

---

[14] More concisely formulated, the TIP system is unique because it is, as far as we know, the only system that is not positioning-based (i.e. is not based on determining positions by means of a GPS and/or an electronic road-map) and at the same time indeed is suited for the fraud-resistantly imposing of continuous fees (such as, for example, a kilometer fee, i.e. distance-related road pricing).

1.19 Description and elucidation of the invention and comparison with related art

This section comprises three subsections. In the first subsection we give some preliminary statements with corresponding elucidations in order to describe and explain many aspects of the invention concisely. In the second subsection we present the formulation of our primary claim. In the third subsection we compare this primary claim with related art.

1.19.1 Preliminary description and elucidation of the invention

In this subsection we give some preliminary statements with corresponding elucidations in order to concisely describe and explain many aspects of the invention. The preliminary statements are formulated as if they are claims. However, all actual claims are formulated in Chapter 19 and our primary claim is presented in subsection 1.19.2 as well.

Preliminary statement 1:

The invention relates to a method for the collection of traffic information by an authority

a) in which use is made of means for supplying information that are present in at least a part of the vehicles,

b) in which traffic information is derived directly or indirectly from the information, or the reception of the information, supplied from vehicles,

c) in which illegitimate tracing of individual persons and/or vehicles is prevented,

d) in which the reliability of the information supplied in or from vehicles is verified in so far as is necessary,

e) in which the authority does not have to trust the fraud resistance of individual components in vehicles other than possibly a small number of agents per vehicle, and

f) in which use of a GPS (Global Positioning System) is not necessary.

Elucidation:

Somewhat shorter (and less precisely) formulated, *Preliminary Statement* 1 describes – a method for – a fraud-resistant traffic information system that prevents illegitimate tracing and that does not require the use of a GPS.

The notion *traffic information* must be interpreted in the broadest sense, as has already been illustrated earlier in this introductory chapter. By traffic information we mean both collective and individual information. By collective information we mean information on collections of several persons or vehicles. Think, for example, of information on traffic flows and/or on average fuel consumption and the like. Individual information concerns information on individual persons and/or vehicles.

Individual information encompasses, among other things, vehicle information, personal information, usage information and circumstantial information. The term vehicle information is described in Chapter 18 and personal information is self-evident. Usage information covers both information on the use of the vehicle (kilometers covered, pollution caused, point in time, etc.; see earlier in this introductory chapter for many more examples) and information on the driver and/or user and/or payer. Circumstantial information covers information on various circumstances during the use, such as, for example, traffic intensity, weather conditions and air pollution. Traffic information also encompasses information on the infrastructure. This kind of

-8 SEP 2003

traffic information is often only disseminated by the traffic information system, but may also be partly collected via the traffic information system.

The term *authority* is used here and in following *preliminary statements* as described earlier in this introductory chapter. Thus, it is possible that the term represents several authorities.

The term *vehicles* must be understood in such a way that it encompasses at least all possible means of conveyance. Note that if one wants to use the TIP system for charging public transportation fares, then in certain cases each passenger must be considered, i.e. act, as a virtual vehicle for the means for supplying information. After all, the supply of the information then might occur before and/or after the entering of the actual, real vehicle of the public transportation system. (For example, when entering and/or exiting the platform.) Although a passenger will then just as well take along with him/her into the actual vehicle the information supplying means in question, the communication with the authority then will not take place from an actual vehicle of the public transporter, but from a passenger (i.e. from a virtual vehicle) outside the actual vehicle.

We have chosen to cover such possibilities by opting for a broad interpretation of the notion of 'vehicle', as explicitly clarified in this elucidation. This choice has been made because it is not easy to include such possibilities explicitly in the formulations without making these again more complicated, less clear and less understandable. As a further illustration we sketch our best attempt. In the formulations (certainly in *Preliminary Statement* 1, but also in a number of other *preliminary statements*), the broader notion of traffic participant(s) should then be used everywhere instead of vehicle(s). This notion must then include, at least, both persons and vehicles.

As a consequence, point c of *Preliminary Statement* 1 then will contain the phrase 'persons and/or traffic participants'. Note that only having 'traffic participants' in point c would be incorrect, as then the essence would be missed as soon as the traffic participants do not stand for persons, but for vehicles for example, as is the case, for example, in road traffic. Yet, the earlier mentioned, indeed correct formulation of point c does have a strange trait. After all, the traffic participants can, like in the above-described example in the context of public transportation, sometimes stand for persons. Therefore, the formulation of point c then actually will include the phrase 'persons and/or persons', which in itself is correct but yet somewhat strange. In any case, with the above example we hope to have elucidated sufficiently the far-reaching scope of the formulation of *Preliminary Statement* 1.

By 'means ... that are *present in* at least a part of the *vehicles*' we understand, among other things, means that are present only during the use of the involved vehicle (e.g. because a person who uses the vehicle has those means on him), as well, of course, as means that have been installed in or at the vehicle involved.

By '*means for supplying* information' we understand not only the means (such as, for example, a transmitter) that are directly involved in the supply, but also means that are indirectly involved in the supply, such as particularly means necessary for the collecting and/or registering of all information necessary to obtain the information to be supplied. For example, these means can also include a receiver. For, assume that an agent (see below) is used for the supply to an authority of reliable information on, say, the kilometer counter value [alternative translation: odometer reading (see Section 7.2)], and that the agent now and then verifies the precision of the kept kilometer counter values by means of reliable information supplied from the out-

- 8 SEP 2003

side world via a transmitter, say, reliable information on the involved vehicle's speed at a certain moment. (See Section 16.7.) Then the required receiver in that vehicle belongs to the means in question. At least all means being mentioned in the enumeration given in Chapter 5 of possibly required elements and/or pieces of equipment, can belong to the means for supplying present in a vehicle.

The *information* to be supplied encompasses at least all information from which traffic information in the broadest sense (see above) can be derived directly or indirectly. Of course, the information supplied from an individual vehicle in our context generally will relate to said one vehicle and/or said one vehicle's near environment, and often will itself already be a form of individual traffic information. Think, for example, of information on that vehicle, about the use of that vehicle and/or about the circumstances when using that vehicle. In any case, in principle it may concern all information that can be collected in an individual vehicle (and thus can be supplied from that vehicle).

The traffic information can be derived from *the contents* of the messages sent from vehicles or from *the reception*. With the formulation '... from the information, or the reception of the information, ...' we wish to emphasize this. The directly or indirectly derivable information thus also covers, for example, information that can be derived from one or more of the following observations: 1) that a message, or a certain message, has been received at all, 2) that a message, or a certain message, has been received at a certain location, 3) that a message, or a certain message, has been sent from a certain location, and/or 4) that a message, or a certain message, has been received at a certain point in time.

The notion of *illegitimate tracing* has already been mentioned in this introductory chapter and is treated extensively in Chapter 3. Thus here it concerns privacy protection in relation to movement patterns. Note that the restrictive qualification 'illegitimate' implies that prevention of legitimate tracing of persons and/or vehicles is not required[15]. We consider the tracing – in a limited degree – of persons and/or vehicles of which the identity, or whose identity respectively, cannot be tracked down, to be legitimate. So, in case of a traffic information system using the method described in this *preliminary statement* tracing really can be permitted, as long as the identities involved cannot be tracked down. Tracing by circumvention of the traffic information system cannot be prevented, of course. Thus, the word '*prevent*' here must be interpreted particularly as 'not make it practically feasible' or as 'impede to a high degree'.

The formulation 'information supplied *in or from* vehicles' has been chosen because verifications on the reliability can be performed not only from a distance, i.e. outside the vehicles, but possibly also – fully or partly – in the vehicle by an agent. (More will be said below about the notion of an agent.) If so, the information supplied to an agent in the vehicle is – fully or partly – verified and the agent then takes care of the supply of – more – reliable information from the vehicle to the authority (or the rest of the authority) in the outside world.

---

[15] An alternative formulation for clause c is '... ... *can be* prevented.' However, because an operational system in general will meet, or have to meet, the legal requirements, it may be assumed that unprevented – kinds of – tracing are legitimate. Therefore, both formulations boil down to the same thing.

-8 SEP 2003

As has been explained already in this introductory chapter, the invention is characterized by, among other things, the way in which '*the reliability of the information* supplied in or from vehicles *is verified* in so far as is necessary'. As a further elucidation of what has already been mentioned in the previous paragraph, we present here once more and explicitly the characteristic ways by which verifications can be performed. Either 1) information is transmitted from a vehicle – almost – continuously and the transmitted information is then spot-checked on correctness by the authority outside the vehicle on the basis of independent observations/measurements (see also *Preliminary Statement* 8). Or 2) information is – almost – continuously supplied in the vehicle to – at least – one agent that now and then (in a random sampling way) comes into contact with a part of the authority in the outside world via a transmitter and/or receiver, and then, based on independent observations/measurements, verifications occur, either a) in the vehicle by the agent, which is informed by the involved part of the authority in the outside world regarding the independently ascertained values, or b) outside the vehicle by a part of the authority that compares the independently determined values with the values reported from the vehicle by the involved agent via a transmitter, which are based on the information supplied to him in the vehicle. (Hybrid forms are also possible; see, among others, *Preliminary Statements* 8 through 11 and the elucidation to these *preliminary statements*.)

With respect to the checking of the reliability of information, we have added the restriction '*in so far as is necessary*', mainly because it is not necessary to verify all information in order to attain – sufficient – fraud resistance. Herewith we do not only aim at the fact that checks are usually performed on random samples, but in particular also at the fact that correctness of all information does not have to be vital. As illustration and clarification of this last remark, we point out the possibility (mentioned in Chapter 8) of letting only identifications or semi-identifications be transmitted from – at least a part of – the vehicles in order to be able to derive information on traffic delays. In this example, it is in general not necessary to check the correctness of the transmitted identification or semi-identification of each vehicle. After all, the desired information usually can be obtained even if the percentage of incorrect identifications or semi-identifications supplied is substantial. Furthermore, most traffic participants then generally will have no interest in supplying incorrect information.

For a further elucidation to the *fraud resistance of individual components* we refer to Chapter 4. Means in the vehicle, such as, for example, transmitters, receivers, sensors, meters, counters and connections, thus do not have to be physically protected against fraud (so far as the authority is concerned), i.e. do not have to be fraud-resistant individually.

For the notion of *agent* we primarily refer to the description given earlier in this introductory chapter. Note that a component being fraud-resistant as seen from the viewpoint of the authority is called an agent only if that component now and then actively performs a task in a vehicle on behalf of the authority. So, a passive component, such as, for example, a magnetic strip or a stamped chassis number, cannot fall under this notion. Even not if, for example, the chassis number has been applied to the chassis or bodywork in such a way that it really is considered by the authority to be sufficiently fraud-resistant. For a further clarification of the notion of agent we refer to elsewhere in this introductory chapter and to Chapters 16 through 18.

With '*a small number*' we knowingly are somewhat vague, for one might use unnecessarily many agents. The most prominent numbers covered here are 0, 1 and 2. These three possible numbers are explicitly expressed in *Preliminary Statements* 8, 9 and 10 respectively.

The word '*possibly*' is intended to express extra clearly that also the absence of agents (i.e. zero agents) lies within the scope of the description.

The words '*not necessary*' are used to express that the use of a GPS is not necessary, but also is not excluded at all. A GPS can, for example, be used to determine on behalf of the user in which tariff zone the vehicle is located (in other words, to enable determination of the locally valid tariff). Also, a sufficiently accurate GPS might be used to keep (without using a sensor on the drive shaft) a kilometer counter and/or speedometer. An important point is that in case of the TIP system no information on successive positions of the vehicle needs to be given to the authority (including also an agent), let alone frequently. With existing traffic pricing systems based on the use of a GPS and/or an electronic road map, i.e. with existing positioning-based systems, the authority (or actually, an agent of the authority) really must frequently get information on successive positions so that, as a consequence, the potential to trace is readily available by definition. As possible abuse of position data for illegitimate tracing can also occur surreptitiously (for example, by means of so-called covert channels), there is always the question of a serious privacy threat (or a serious threat to privacy protection) in such systems.

In a preferred embodiment of a method according to the invention, reliable information can be collected about one or more aspects, among which should at least be understood individual information on, among others, the distance covered, the location, the date, the point in time, the brand, the model, the year of manufacture, the gearbox type, the engine type, the gear engaged, the engine speed, the speed, the speed changes, the kind of fuel used, the fuel consumption, the noise production and/or the environmental pollution caused, and collective information on, among other things, the traffic intensity, tailbacks, the fuel consumption, the noise production and/or the environmental pollution caused. (This is *Preliminary Statement* 2.)

Elucidation:

With this *preliminary statement* we try to indicate the broad scope of the TIP system with respect to the kinds of information that can be collected and, as far as necessary, be verified on reliability. Note, however, that this always concerns information that *can* be collected *in principle*. So, it is not true that every TIP system actually has to, or has to be able to, collect and verify all mentioned kinds of information. The notions of individual and of collective information used here have been introduced in the elucidation to *Preliminary Statement* 1. The more precise meaning of the concisely formulated enumeration has already been made clear, or more clear, earlier in this introductory chapter by means of a more extensively formulated enumeration with some corresponding elucidation. To be quite on the safe side, we mention here once more explicitly that the enumeration is not exhaustive. Note that the collective information can be divided [alternative translations: split up, itemized], if required, according to one or several of the aspects, whether mentioned or not.

In a further preferred embodiment of a method according to the invention, the tracking of traffic flows and the determination of traffic delays can be performed automatically and in a privacy-friendly way. (This is *Preliminary Statement* 3.)

-8 SEP 2003

Elucidation:

With the tracking of traffic flows we particularly mean also the gaining of an insight into how traffic flows split up and join. It is thus necessary to be able to track individual vehicles in the traffic flow. Both tasks mentioned can be performed with the aid of semi-identifications transmitted from vehicles. (See also the next *preliminary statement*.) Note that the aspect of privacy-friendliness in fact is already included in *Preliminary Statement* 1 as well.

In a further preferred embodiment of a method according to the invention, use is made of one or more semi-identifications. (This is *Preliminary Statement* 4.)

Elucidation:

The term *semi-identification* here stands both for a semi-identification process and for a semi-identifying datum (or a semi-identifying combination of data). These notions are treated in Chapter 15. Semi-identifications can be used, for example, for performing trajectory speed checks in a privacy-friendly way, for inspections of the precision of counters, and for certain tasks belonging to the denotation 'traffic management', such as, for example, performing traffic census, tracking traffic flows, determining the average speed of traffic flows, determining speed differences between individual vehicles in a traffic flow, determining the distances between vehicles, detecting incipient tailbacks, detecting tailbacks and/or determining traffic delays due to tailbacks. Indirectly, this is, for example, also useful for traffic control and for determining and/or planning the need for expansion of the infrastructure.

In a further preferred embodiment of a method according to the invention, illegitimate tracing is prevented by using at least one organization that is independent of the authority. (This is *Preliminary Statement* 5.)

Elucidation:

This *preliminary statement* not only encompasses the use of a hunter and/or intermediary, but also, for example, the use of an organization that provides for the possibility of protecting privacy by means of a certain indirect identification. The indirect identification then concerns an identification that has been supplied semi-anonymously. (See Chapter 13. The word identification here stands for an identifying combination of data, such as, for example, an identification number.) To be quite on the safe side, the use of a hunter and/or an intermediary is also covered by two separate, specific *preliminary statements*, namely *Preliminary Statements* 6 and 7.

In a further preferred embodiment of a method according to the invention, one or more hunters are used for at least a part of the communication between vehicles and the authority. (This is *Preliminary Statement* 6.)

Elucidation:

The notion of *hunter* is described in Chapter 13 (and particularly at the end of that chapter). A hunter is an organization that controls at least a part of the transmitting and/or receiving devices in the outside world (i.e. outside the vehicles) in aid of the communication between vehicles and – the rest of – the traffic information system, and contributes to keeping the position of a person or vehicle as secret as possible, in particular at the moment of reception of a message from that vehicle. Primarily we here allude to a 'pure' hunter (see Chapter 13), but secondarily also to a hunter that does perform at least a part of the tasks of an intermediary as well.

In a further preferred embodiment of a method according to the invention, one or more intermediaries, acting as go-between during communication, are used for at least a part of the communication between vehicles and the authority. (This is *Preliminary Statement* 7.)

Elucidation:

The notion of *intermediary* is described in Chapter 13 (and particularly at the end of that chapter). An intermediary is an organization that is independent of the authority and that for the benefit of privacy protection acts as a go-between during the communication from vehicles with the authority.

In a further preferred embodiment of a method according to the invention, in at least a part of the vehicles, even during usage, no agent is required. (This is *Preliminary Statement* 8.)

Elucidation:

For the vehicles without agent, the possibly required verifications must then be performed from a distance, i.e. outside the vehicles concerned. This *preliminary statement* thus covers the case that for – at least a part of – the vehicles the approach using exclusive remote checks is being used.

In a further preferred embodiment of a method according to the invention, in at least a part of the vehicles, during usage, one agent is required. (This is *Preliminary Statement* 9.)

Elucidation:

See Chapter 16 and particularly Sections 16.12 and 16.14. Note that here, for example, it has not been laid down that the agent should perform verifications. If the agent does perform verifications, then still the agent does not necessarily have to perform all verifications. (See also the elucidation to *Preliminary Statement* 11.)

In a further preferred embodiment of a method according to the invention, in at least a part of the vehicles, during usage, two agent are required. (This is *Preliminary Statement* 10.)

Elucidation:

See the elucidation to *Preliminary Statement* 9.

In a further preferred embodiment of a method according to the invention, all or a part of the verifications of the reliability of the information supplied from a certain vehicle are performed fully or partly outside that vehicle, i.e. from a distance. (This is *Preliminary Statement* 11.)

Elucidation:

This *preliminary statement* is particularly intended to cover *explicitly* all possibilities whereby verifications occur that are performed fully or partly from a distance. Implicitly, at least a number of these possibilities were covered already. For the sake of clarity we here explicitly list four of the total number of possible situations: 1) the possibility that *all* verifications in relation to a certain vehicle are performed fully from a distance (this possibility actually was already covered indirectly, or implicitly, by *Preliminary Statement* 8), 2) the possibility that *all* verifications are performed fully by one or more agents (this possibility was covered already by the *Preliminary Statements* 1, 9 and 10, but note that the *Preliminary Statements* 9 and 10 also cover cases in which, for a certain verification, agents take care of only a part of that verification), 3) the possibility that in relation to one certain vehicle a certain verification is performed *fully* from a distance and also a certain verification is performed *fully* by one or more agents, and 4) the possibility that a certain veri-

fication is performed *partly* from a distance and *partly* by an agent. For an example of the last-mentioned possibility see Chapter 16, and in particular Section 16.3 and a number of sections following that section. This *preliminary statement* is intended to explicitly cover possibility 1 and in particular also the possibilities 3 and 4.

In a further preferred embodiment of a method according to the invention, information is collected on the fuel consumption of individual vehicles. (This is *Preliminary Statement* 12.)

Elucidation:

Information on fuel consumption includes both information on the speed of fuel supply (i.e. on the value indicated by a fuel consumption meter) and about the reading of a fuel meter (i.e. of a fuel consumption counter). The information in question can be collected, for example, in order to be able to derive data about the fuel consumption as actually realized by vehicles, analyzed or not into e.g. brand, model, year of make, gearbox type, engine type, speed, speed change, gear engaged, engine speed, engine temperature, air humidity, outside temperature, and the like. Or it can be collected, for example, to be used, or also used, for traffic pricing (see *Preliminary Statement* 18). Note that the collected information can, if desired, be verified on reliability.

In a further preferred embodiment of a method according to the invention, information is collected on environmental pollution caused by individual vehicles. (This is *Preliminary Statement* 13.)

Elucidation:

This kind of information can be collected, for example, to obtain a better view of the total environmental pollution caused by motorized vehicles or, for example, to use this information – also – for traffic pricing (see *Preliminary Statement* 18). Note that the collected information can, if desired, be verified on reliability.

In a further preferred embodiment of a method according to the invention, information is collected on noise caused by individual vehicles. (This is *Preliminary Statement* 14.)

Elucidation:

This kind of information can be collected, for example, to get a better view of the noise nuisance, or the traffic-noise, on certain road sections or, for example, to use this information – also – for traffic pricing (see *Preliminary Statement* 18). See, for example, Sections 15.8 and 18.4. Note that the collected information can, if desired, be verified on reliability.

In a further preferred embodiment of a method according to the invention, information is collected on the gear engaged in individual vehicles. (This is *Preliminary Statement* 15.)

Elucidation:

Note that the collected information can, if desired, be verified on reliability. See also *Preliminary Statement* 28. This kind of information can be collected, for example, to use this information – also – for traffic pricing (see *Preliminary Statement* 18).

In a further preferred embodiment of a method according to the invention, information is collected on the engine speed of individual vehicles. (This is *Preliminary Statement* 16.)

Elucidation:

- 8 SEP 2003

Note that the collected information can, if desired, be verified on reliability. See also *Preliminary Statement* 28. This kind of information can be collected, for example, to use this information – also – for traffic pricing (see *Preliminary Statement* 18).

In a further preferred embodiment of a method according to the invention, information is collected on certain counters associated with individual vehicles or persons. (This is *Preliminary Statement* 17.)

Elucidation:

The *counters* can be of all kinds. Think, for example, of kilometer counters, revolution counters, and the like, but also of counters regarding fuel consumption, noise production, environmental pollution, usage rights, levying points, and the like. This kind of information can be collected, for example, to get a better view of the total volume of the traffic with certain kinds of motorized vehicles or, for example, to use this information – also – for traffic pricing (see *Preliminary Statement* 18).

In a further preferred embodiment of a method according to the invention, the collected information is used, or is also used, for imposing a traffic fee. (This is *Preliminary Statement* 18.)

Elucidation:

The wide sense of the notion *traffic fee* has already been described earlier in this introductory chapter. Note that all three kinds of pricing mentioned in Chapter 2, namely open and closed tolling and continuous pricing, are included here. For a number of examples of tariff functions we refer to Chapter 7. See *Preliminary Statement* 2 and the earlier text in this introductory chapter for examples of – verifiable – quantities that can be used as parameter(s) of a tariff function. See also *Preliminary Statements* 19 and 20.

Note: By *tariff function* we mean the same as price function (see, for example, Chapter 7).

In a further preferred embodiment of a method according to the invention, the tariff employed can be related to one or more of the following aspects: the distance covered, the location, the date, the point in time, the traffic intensity, the brand, model, year of manufacture, gearbox type, engine type, the gear engaged, the engine speed, the speed, the speed changes, the kind of fuel, the fuel consumption, the noise production and the environmental pollution caused. (This is *Preliminary Statement* 19.)

Elucidation:

On the basis of *Preliminary Statements* 2 and 18, this *preliminary statement* is rather obvious. To be quite on the safe side, we have chosen to formulate this *preliminary statement* explicitly also. See, for example, the text earlier in this introductory chapter for a somewhat more extensively formulated enumeration with – a part of – the corresponding elucidation. To be quite on the safe side, we here emphasize once more explicitly that the enumeration is not exhaustive. (See possibly also the elucidation to *Preliminary Statement* 2.)

The above is valid for open and closed tolling as well as for continuous pricing.

In a further preferred embodiment of a method according to the invention, the collected information is used, or is also used, for imposing a continuous fee. (This is *Preliminary Statement* 20.)

Elucidation:

A *continuous fee* is a specific form of a traffic fee. The notion of continuous fee [alternative translation: continuous pricing] is treated in Chapter 2. The continuous pricing can be based, for example, on a kilometer counter, a fuel consumption counter, a noise production counter, an environmental pollution or pollution

equivalents counter and/or any other traffic fee counter. In this way one thus can charge, for example, for all distances traveled, all fuel consumption, all noise caused, all environmental pollution caused, and the like. For a number of examples of tariff functions (i.e. price functions), we refer to Chapter 7.

In a further preferred embodiment of a method according to the invention, at least a part of the communication from a certain vehicle with an authority that collects, verifies and/or disseminates traffic information, takes place via a transmitting means present in and/or attached to that vehicle and a receiving means outside that vehicle. (This is *Preliminary Statement* 21.)

Elucidation:

This *preliminary statement* describes that all or part of the communication between vehicle and an authority in the outside world can take place via transmitters and receivers. The passage 'at least a part' has a double function, as it emphasizes: 1) that here the communication in one direction, viz. from vehicle to the outside world, is concerned, and 2) that not all communication has to take place via the means for transmitting and receiving.

In a further preferred embodiment of a method according to the invention, at least a part of the communication from a certain vehicle with an authority that collects, verifies and/or disseminates traffic information, takes place via a transmitting means outside that vehicle and a receiving means present in and/or attached to that vehicle. (This is *Preliminary Statement* 22.)

Elucidation:

For this *preliminary statement* the same is valid as for the previous one, on the understanding that now the communication from the outside world to the vehicle is concerned.

In a further preferred embodiment of a method according to the invention, at least a part of the means outside the vehicles for transmitting and/or receiving are mobile. (This is *Preliminary Statement* 23.)

Elucidation:

This *preliminary statement* speaks for itself, on the understanding that the meaning of mobile should be taken in a dual sense, namely both in the meaning of movable and in the meaning of being in motion (say, moving). Thus, this *preliminary statement* covers, for example, 'reading out' vehicles from a moving patrol car. Performing verifications from a moving patrol car will be covered explicitly by *Preliminary Statement* 30.

In a further preferred embodiment of a method according to the invention, dissemination of traffic information by an authority is involved or also involved. (This is *Preliminary Statement* 24.)

Elucidation:

This *preliminary statement* describes that the traffic information system concerned in this *preliminary statement* is suited, or also suited, for the dissemination of traffic information. Note that traffic information also covers information on the infrastructure. Think, for example, of entry prohibitions, speed limits and temporarily mandatory alternative routes (i.e. detours). Also the information that is sent to a vehicle, for example for navigation or for the benefit of verifications in the vehicle by an agent (think of the earlier treated position and/or speed data), is covered by our wide notion of traffic information.

In a further preferred embodiment of a method according to the invention, semi-identifications derived from counter values are used. (This is *Preliminary Statement* 25.)

Elucidation:

The counter in question can, for example, be a kilometer counter, a consumption counter or a traffic fee counter. The only thing being essential is that the correct progress of the counter value in question can be determined or predicted externally (i.e. from a certain distance outside the vehicle) with sufficient accuracy. The counter in question may belong to the vehicle concerned or to the user or payer concerned. See also Chapter 15.

In a further preferred embodiment of a method according to the invention, semi-identifications derived from the registration number of each vehicle concerned are used. (This is *Preliminary Statement* 26.)

Elucidation:

See also Chapter 15 and in Section 15.3 in particular.

In a further preferred embodiment of a method according to the invention, semi-identifications, for each vehicle randomly chosen from a set of elements, are used. (This is *Preliminary Statement* 27.)

Elucidation:

See also Chapter 15 and Section 15.3 in particular.

In a further preferred embodiment of a method according to the invention, the information supplied in or from a vehicle is verified on reliability and the information verified (and supplied) concerns at least information on one of the following aspects: the kilometer counter value, the speed, the gear engaged, the engine speed, the fuel consumption, the noise production and/or the environmental pollution caused. (This is *Preliminary Statement* 28.)

Elucidation:

For verification one needs external ascertainment of the right information. Note that kilometer counter values and speed indications are related to each other and thus are, in a certain sense, mutually interchangeable data. (See also Section 11.10.) Of course, something similar is valid for a fuel consumption meter and counter, a noise production meter and counter, and an environmental pollution meter and counter. Revolution counter generally denotes both 'rotational speed meter' and 'cumulative revolution counter'. How the kilometer counter value and/or the speedometer indication can be verified is explained in Chapters 11 and 16. In other words, externally ascertaining the length of a certain trajectory, or of the speed at a certain moment, is easy and well-known. The gear engaged can externally be ascertained (and thus verified) via speed measurement(s), speed change measurement(s) and directional noise production measurement(s), while reliable information on the vehicle type is also required. The manner in which the engine speed and the [momentary] fuel consumption can be determined externally is described in Section 11.7. In Section 11.8 it is explained how the noise production can be ascertained. The use of derived information was already elucidated earlier in this introductory chapter.

In a further preferred embodiment of a method according to the invention, an agent performs verifications in the vehicle with the help of externally ascertained, reliable information supplied to it. (This is *Preliminary Statement* 29.)

- 8 SEP 2003

Elucidation:

See Chapter 16. The manner in which the required reliable, i.e. correct, information can be ascertained externally has already been elucidated with *Preliminary Statement* 28 for a number of kinds of information. For e.g. location, date and point in time, the external ascertainment needs no further elucidation. The manner in which forwarded, reliable position or speed data can be used for verifications on kilometer counter values and speed indication, is described in Chapter 16. Checks on speed changes can be performed similarly. (See also Section 11.10.) Verifications of, for example, engine speed, noise production, fuel consumption and the like are also sufficiently described elsewhere in the text. The externally ascertained and reliable information supplied to the agent may also comprise an algorithm for computing derived information. For further elucidation regarding the use of derived information we refer, for example, to Section 1.14 of this introductory chapter.

Note that this *preliminary statement* also covers continuous surveillance of traffic behavior (such as, for example, the continuous speed checks already mentioned in section 1.3.). See also Section 16.8 and point 5 in Section 18.1.

In a further preferred embodiment of a method according to the invention, verifications are performed from mobile checkpoints. (This is *Preliminary Statement* 30.)

Elucidation:

Here we mean with mobile not only movable, but in particular also moving. This *preliminary statement* thus covers, for example, checking from moving patrol cars. Flying checkpoints may be attractive because of, for example, the surprise effect that can be attained.

In a further preferred embodiment of a method according to the invention, trajectory speed checks are performed in a privacy-friendly way. (This is *Preliminary Statement* 31.)

Elucidation:

By *privacy-friendly* we mean that identification of the person (or payer) and/or of the vehicle in question will take place only for those vehicles that have exceeded the speed limit. The meaning of payer will be treated in Chapter 5.

In a further preferred embodiment of a method according to the invention, a correct indication of time is disseminated and in at least a part of the vehicles at least one clock will be adjusted automatically, in particular when passing from one time zone to another or when changing from daylight saving time to standard time or vice versa. (This is *Preliminary Statement* 32.)

In a further preferred embodiment of a method according to the invention, a quota system is used, in which the consumption rights are tradable or not. (This is *Preliminary Statement* 33.)

Elucidation:

Consumption rights also stands for usage rights and 'pollution rights'. Usage rights can be expressed, for example, in kilometers and 'pollution rights' can be expressed in some environmental pollution unit.

In a further preferred embodiment of a method according to the invention, deviating and possibly not or no longer correctly functioning vehicles and/or vehicle equipment are tracked down. (This is *Preliminary Statement* 34.)

Elucidation:

For the notion of vehicle equipment, see Chapter 5. The deviation can be caused, for example, by a defect, by wear, by bad tuning or by an attempt to defraud.

In a further preferred embodiment of a method according to the invention, vehicles can be tracked down upon authorized request. (This is *Preliminary Statement* 35.)

Elucidation:

See Chapter 12.

In a further preferred embodiment of a method according to the invention, software can be distributed, installed, and/or put into operation via the traffic information system. (This is *Preliminary Statement* 36.)

In a further preferred embodiment of a method according to the invention, an agent fully or partly verifies the reliability of a measuring instrument or counter in the vehicle concerned. (This is *Preliminary Statement* 37.)

Elucidation:

See Chapter 16. There we show that checking of, for example, a kilometer counter can also be performed partly by an agent.

In a further preferred embodiment of a method according to the invention, use is made of agents consisting of a chip with a processor and memory that, at least for a part, is sufficiently protected against reading of the data stored therein and against modification of such data and/or against modification of the software used by that chip. (This is *Preliminary Statement* 38.)

Elucidation:

Although software in principle can be considered to be data as well, it has been mentioned here separately, because the software does not have to be protected against reading. For the data protected against reading and modification (and thus also against writing) think of, for example, counter values and/or cryptographic keys.

In a further preferred embodiment of a method according to the invention, real-life data are collected on certain performances of vehicles under certain usage conditions and said data are, or are not, processed into information on certain performances of certain groups of vehicles under certain usage conditions. (This is *Preliminary Statement* 39.)

Elucidation:

With usage conditions we mean here, for example, all aspects related to usage information and to circumstantial information, both of which categories have been described in the elucidation to *Preliminary Statement* 1. Think, for example, of the collecting of data concerning fuel consumption and processing these data into information on the fuel consumption level under certain usage conditions, such as in case of a certain speed, gear engaged, acceleration, outside temperature, and the like.

In a further preferred embodiment of a method according to the invention, the data collected in practice are used for finding/determining an algorithm for computing derived information. (This is *Preliminary Statement* 40.)

Elucidation:

- 8 SEP 2003

An algorithm can, for example, be expressed in any natural or computer language or, for example, as one or more tables. It can be used, for example, for verifications or for use in new 'measuring' instruments.

In a further preferred embodiment of a method according to the invention, an algorithm for computing derived information is used to determine the fuel consumption and/or the noise production of an individual vehicle, whether or not to be used for the benefit of checking. (This is *Preliminary Statement* 41.)

In a further preferred embodiment of a method according to the invention, an algorithm for computing derived information is used to determine the quantity of – a certain form of – environmental pollution caused by an individual vehicle. (This is *Preliminary Statement* 42.)

In a further preferred embodiment of a method according to the invention, cruise control equipment in a vehicle makes use of information on speed limits that has been disseminated outside the vehicle and has been received by equipment in the vehicle. (This is *Preliminary Statement* 43.)

Elucidation:

The information disseminated on a speed limit may exist of an absolute indication of the speed limit or of the relative change of the new speed limit with respect to the previous one. (In the latter case it concerns the difference in speed limits on the borderline between two connected areas that each have their own speed limit.) Cruise control equipment may – upon request of the driver – use the information on the locally valid speed limit for automatic respecting of speed limits.

In a further preferred embodiment of a method according to the invention, the information collected and/or disseminated by means of the traffic information system is used for calibrating measuring instruments. (This is *Preliminary Statement* 44.)

Elucidation:

See Section 12.1. This *preliminary statement* does not only cover calibration of instruments whether in a vehicle or outside the vehicles, but also covers the case of mutual [alternative translation: reciprocal] calibration. Think, for example, of calibration of clocks, outside temperature meters, air humidity meters, noise or noise production meters, speedometers and kilometer counters. In case of the latter two examples, one thus can banish the inaccuracy due to tire wear.

In a further preferred embodiment of a method according to the invention, an agent is used, or also used, for fraud-resistant identification of the vehicle in which that agent, whether attached in a fraud-resistant way or not, has been installed. (This is *Preliminary Statement* 45.)

In a further preferred embodiment of a method according to the invention, the correctness of the counter value or counter values supplied is fully or partly remotely spot-checked. (This is *Preliminary Statement* 46.)

Elucidation:

That counters can be fully verified remotely, if desired, will be illustrated in Chapter 11. That counters can be partly verified remotely, if desired, will be illustrated in Chapter 16 using kilometer counters as example. Think, in particular, of various verification aspects, such as verification of precision and verification of monotony.

In a further preferred embodiment of a method according to the invention, audio-visual means have been installed in a vehicle to render at least a part of the information. (This is *Preliminary Statement* 47.)

In a further preferred embodiment of a method according to the invention, at least a part of the disseminated information is used, or also used, for navigation. (This is *Preliminary Statement* 48.)

The invention also relates to a traffic information system using a method according to the invention. (This is *Preliminary Statement* 49.)

The invention also relates to a traffic information system according to *Preliminary Statement* 49 that is prepared for adaptations and extensions. (This is *Preliminary Statement* 50.)

The invention also relates to a vehicle suited for a method, or for use with a method, according to the invention. (This is *Preliminary Statement* 51.)

The invention also relates to an agent suited for a method, or for use with a method, according to the invention. (This is *Preliminary Statement* 52.)

Elucidation:

An agent is a hard- and/or software component that is considered by the authority to be fraud-resistant.

The invention also relates to a hardware and/or software component suited for use as vehicle-related processor for a method according to the invention. (This is *Preliminary Statement* 53.)

Elucidation:

This component will – very likely – be some data-processing device that consists of a processor with memory and software and that does not have to be fraud-resistant. The vehicle-related processor is primarily intended for performing tasks on behalf of the holder (and possibly also on behalf of the user) of the vehicle. It might perform, or also perform, certain tasks on behalf of the authority, at least if the authority allows those tasks to be performed on behalf of itself by a not fraud-resistant component, i.e. if the authority does not adhere to a really good protection against fraud. See, for example, Chapters 5 and 17.

The invention also relates to a user card suited for a method, or for use with a method, according to the invention. (This is *Preliminary Statement* 54.)

Elucidation:

The notion of user card has a wide meaning here. A user card thus also includes, for example, a consumption card. See Chapter 5.

The invention also relates to a roller test bench for the further inspection of the functioning of vehicle equipment that is used, or is also used, for the sake of a method according to the invention or for the sake, or also for the sake, of a traffic information system according to the invention. (This is *Preliminary Statement* 55.)

The invention also relates to a reliable taximeter in which use is made of a method according to the invention. (This is *Preliminary Statement* 56.)

Elucidation:

The adjective 'reliable' here does not only concern the fraud resistance of the equipment itself, but particularly also the verification of the correctness of – at least a part of – the data supplied. (See Chapter 18.)

The invention also relates to a reliable tachograph in which use is made of a method according to the invention. (This is *Preliminary Statement* 57.)

Elucidation:

The adjective 'reliable' here does not only concern the fraud resistance of the equipment itself, but particularly also the verification of the correctness of – at least a part of – the data supplied. (See Chapter 18.)

The invention also relates to a reliable 'black-box' in which use is made of a method according to the invention. (This is *Preliminary Statement* 58.)

Elucidation:

The adjective 'reliable' here does not only concern the fraud resistance of the equipment itself, but particularly also the verification of the correctness of – at least a part of – the data supplied. (See Chapter 18.)

I.19.2 Our primary claim

The invention claimed in this patent application concerns:

Method for the collection of traffic information by or on behalf of an authority

a) in which during the traffic participation of a vehicle involved:

1) vehicle equipment supplies traffic information to one or more processors present in said vehicle

2) said processor or processors process said information and keep record of certain traffic information on the use of said vehicle

3) said processor or processors transmit certain traffic information to outside said vehicle by means of a transmitter present in said vehicle

b) that is characterized by the combination of properties that:

1) the traffic information collected by or on behalf of the authority includes values of counters that are associated with individual vehicles and/or persons and that during traffic participation are kept up-to-date by said processors in the vehicles involved,

2) during the traffic participation of a vehicle involved said processor or processors transmit certain traffic information continually, and at least at a prescribed rate, to outside said vehicle by means of a transmitter with a prescribed range

In order to make said information available to outside said vehicle in such a way that the authority has the ability to gain access to said transmitted information at any desired moment by placing a receiver within the range of the transmitter of said vehicle

3) remote spot-checks by surprise are used to verify the reliability of the values of said counters

4) such a spot-check by surprise from outside a vehicle being checked comprises

intercepting one or more samples of the traffic information that is continually transmitted from said vehicle during its traffic participation as described in the first half of clause b.2, by means of a receiver that is placed within the range of the transmitter of said vehicle as described in the second half of clause b.2, and

comparing said intercepted sample or samples of the traffic information transmitted from said vehicle

with traffic information concerning said vehicle that has been independently determined at a distance from and outside said vehicle.

Further aspects, details and preferred embodiments of said method are formulated in additional claims. For the formulations of these additional claims we refer to Chapter 19.

1.19.3 Comparison with related art

In this subsection we consider the related art described in patent documents US 5,812,069, US 5,767,505 and DE 43 10 579 A1. For completeness, we mention that the comparisons given below are not exhaustive.

Comparison with US 5,812,069

The patent US 5,812,069 describes a method (and system) for collecting traffic information and forecasting traffic flows at selected locations.

In the case of this method, driving activity sensors continually determine the actual location positions of the vehicles belonging to a certain subset. The actual positions of each such a vehicle are stored as route data. These route data are transmitted at intervals from the vehicle to a traffic computer by means of a transmitter present in the vehicle. The traffic information thus collected is used for forecasting traffic flows at selected locations.

In the method according to this US patent, there is no question at all of verifying the reliability of the collected information, let alone by remote spot-checking by surprise comprising a comparison with independently determined traffic information, as is the case with our invention. Obviously, verifying the reliability of the information collected is important for many applications, such as, for example, traffic pricing.

Furthermore, there is no mention of the collection of any counter associated with an individual vehicle or person and no explicit mention of continual transmission.

Comparison with US 5,767,505

The patent US 5,767,505 describes a method (and system) for traffic pricing by means of virtual toll gates, i.e. a method (and system) for open and/or closed tolling.

In the case of this method, a position determination device located in the vehicle is used to compare continually the actual position of the vehicle with a plurality of predetermined positions of virtual collection points. If a comparison reveals the passing of a virtual collection point, i.e. a virtual toll gate, then a processor in the vehicle calculates the user fee and transmits the calculated user fee to a central point. This US patent also mentions the possibility of reducing the number of transmissions by keeping record of the calculated user fees in a memory located in the vehicle and by only transmitting the calculated user fees to the central point when a predetermined amount of calculated user fees has been stored in the memory.

As a consequence, in the case of this US patent the transmission occurs at most once at each virtual toll gate. Therefore, there is clearly no question at all of transmitting continually and at least at a prescribed rate. After all, it will not happen that each vehicle will pass the virtual toll gates continually and at least at a prescribed rate.

Furthermore, there is no question at all of remote spot-checking by surprise. (Obviously, spot-checking by surprise is beneficial for achieving fraud resistance.) Indeed, this US patent describes the possibility of monitoring/checking by means of monitoring devices placed downstream of the virtual toll gates. However, the vehicles are informed in advance about which virtual toll gates have downstream connected monitoring devices, which means that the vehicles know the locations of checking in advance!

The fact that the method according to US patent US 5,767,505 does not use remote spot-checks by surprise to verify whether the counters (counting the 'added-up user fees') are continually kept correctly, implies that physical protection of certain vehicle equipment, such as the processor in the vehicle, is essential for achieving fraud resistance. In the case of using the continual transmission and the remote spot-checks by surprise of our method, physical protection of vehicle equipment is not of essential importance, i.e. is not necessary. (See e.g. our Section 5.3.)

As a final remark, we mention that the method of this US patent uses virtual toll gates. Therefore, it is only a method for implementing open and/or closed tolling and it is not suitable for continuous pricing. For example, this method does not allow charging for each distance unit actually traveled, let alone a price that depends on the speed with which that distance unit has been traveled. (Cmp. lines 9-16 of our Section 7.3.) An important property of the method of our application is that it is suitable for continuous pricing.

Comparison with DE 43 10 579 A1

The patent document DE 43 10 579 A1 describes a system for spot-checking during traffic participation whether toll has been paid for the passing of a toll gate, i.e. a system for remote spot-checking toll payment in an open tolling system.

In the case of this system, the vehicles are equipped with an On-Board Unit, a transceiver and a chipcard. If a vehicle passes a toll gate, information is exchanged between the toll gate and the processor on the chipcard in said vehicle via the transceiver (and the On-Board Unit) in said vehicle. The chipcard is depreciated with the amount of toll and a proof of payment (i.e. a receipt), which is received from the toll gate, is stored on the chipcard. Verification whether vehicles have paid for toll gates they passed is performed by a separate process of remote spot-checking. A remote spot-check comprises a request-response cycle performed by a – stationary or mobile – checking device to interrogate the vehicle equipment (by means of wireless communication) in order to verify whether a correct receipt for passing the last toll gate is present (or, respectively, whether correct receipts for passing the last few toll gates are present).

In the case of this system, transmission via the transceiver of a vehicle involved occurs only when said vehicle passes an electronic toll gate along the road or when said vehicle is interrogated by a checking device. Therefore, there is clearly no question at all of transmitting continually and at least at a prescribed rate. After all, it will not happen that each vehicle will pass the electronic toll gates and checking devices continually and at least at a prescribed rate.

Furthermore, in the case of the system described in patent document DE 43 10 579 A1 there is a question of collecting proofs of payment (namely, during spot-checking), but there is no question of collecting counter values, let alone of counter values that are associated with individual persons and/or vehicles and that during traffic participation are kept up-to-date in the vehicles involved.

The system described in patent document DE 43 10 579 A1 uses a sort of remote spot-checking. However, note that this remote spot-checking only comprises checking whether the chipcard in the vehicle possesses the right receipts, i.e. whether the chipcard can prove that the fee for passing the last few toll gates has been paid. In the case of the system described in patent document DE 43 10 579 A1 the remote spot-checking is, for example, not used for verifying the monotony and precision of the counter, and thus the reliability of the values of said counter, kept by the processor on the chipcard (i.e., whether the counter values on the chipcard are kept correctly).

The above implies that physical protection of certain vehicle equipment, in particular of the processor on the chipcard, is essential for achieving fraud resistance. In the case of using the continual transmission and the remote spot-checks by surprise of our method, physical protection of vehicle equipment is not of essential importance, i.e. is not necessary. (See e.g. Section 5.3.)

As a final remark, we mention that the system described in patent document DE 43 10 579 A1 uses electronic toll gates along roads and therefore is not suitable for continuous pricing. An important property of the method of our application is that it is suitable for continuous pricing.

1.20 Elucidation to and overview of the further contents

In the following we will treat step by step all kinds of aspects of the TIP system, and in particular also explain how one thing and another work. In our treatment we will concentrate mainly on the use of a TIP system for traffic fees in the case of road traffic and for road pricing more in particular. We do this not only because this is an important application, but also because with this application the manner of verification and privacy protection that is characteristic for TIP systems is demonstrated effectively. After all, protecting privacy and combating fraud are, in the case of road traffic pricing, and of traffic fees more in general, obviously of great importance.

-8 SEP 2003

Now and then aspects and applications that are not or not directly related to road traffic pricing or, more generally, to traffic pricing, will be addressed in passing.

Now and then, we will use a specific example and sometimes mention a number of possible variations. The given examples and variations serve, as already remarked earlier, as an illustration only and should not be understood as imposed restrictions. As already remarked in a footnote, we also often speak of *the* TIP system, although it actually concerns a class of many systems with certain characteristics.

Our explanation occurs more or less in two phases by describing in first instance an approach without, and then – not until almost at the end – one with use of agents. Unintendedly, our explanation perhaps conceals – whether or not partly due to doing so – somewhat that there is a whole range of possibilities to realize a TIP system with the aid of the described techniques, and that for the various realizations elements of both more explicitly described approaches might be combined.

For further orientation on the complete text, we present here an overview of all chapters:

1. Introduction
2. Kinds of fees and tariff systems
3. Tracing
4. Fraud resistance
5. Equipment
6. Cryptography
7. Accounting
8. Use of a transmitter
9. Security of messages
10. Identification numbers in messages
11. Checks
12. Use of a receiver
13. Privacy protection
14. Identification
15. Semi-identification and its applications
16. The approach using agents
17. Preparation for 'growth' of the system
18. TIP systems
19. Claims

2 Kinds of fees and tariff systems

One can distinguish between several kinds of fees or tariff systems. In this text, we use a classification in which – at the least – a distinction is made between open tolling, closed tolling and continuous pricing.

In the case of *open tolling* [alternative translation: pass-by fees], the fee is charged based on the passing of certain borderlines, whether or not in the direct environment of a certain point or tolling point[16]. Examples are im-

[16] The essential point is that only one measuring point is of interest.

-8 SEP 2003

port and export taxes on traffic of goods when passing national borders, lock and bridge fees for ships, and the charging of tolls for tunnels and bridges in the case of road traffic. There is also a question of open tolling in the case of certain zone-related payment systems, which occur, for example, in several forms of public transport. In the case of the zone-related payment systems alluded to, the tariff depends on the number of borderlines between zones that one passes, so that clearly one can speak of open tolling [alternative translation: pass-by fees]. However, one usually also pays for transport within one zone, thus in which case no borderline between zones is passed at all. In this case, however, one does indeed pass a borderline, viz. when entering the transport system[17], in particular when entering the vehicle or the platform.

In the case of *closed tolling* [alternative translations: 'trajectory' fees, pass-through fees], the fee is levied for traveling some trajectory or another from a certain starting-point to a certain end-point, the precise trajectory, if it can be chosen at all, not playing any role[18]. Examples are certain tariff systems used for public transport and certain tolling systems in which for each passenger or for each vehicle both the place of entrance to the transport system or to a road or road network respectively, and the place of exit from said system or network respectively, are used to determine the correct fee. If one can choose from several routes between the point of entrance and the point of exit, then this choice should have no influence on the fee. If the chosen route does have influence, then usually there is a question of some form of open tolling or sometimes of some form of continuous pricing.

In the case of *continuous pricing* [alternative translation: integral levying], the complete 'consumption' [alternative translation: 'usage'] or the complete 'turnover', expressed, for example, in kilometers, liters of fuel, minutes, Dutch guilders or some environmental pollution unit, is charged. Possible examples are income tax, sales tax and fuel excise-duties[19].

As already somewhat exemplified by the above, it is not always easy to classify correctly a tariff system as an open tolling, closed tolling or continuous pricing system. Nevertheless, we assume that one thing and another are sufficiently clear for our purpose, viz. the description and elucidation of various aspects of the TIP-system.

3 Tracing

As has been remarked in the introduction, the TIP system is characterized, among other aspects, by the way in which provisions can be made for the property [alternative translation: attribute] that – when collecting and/or verifying information on persons and/or vehicles – illegitimate tracing of individual, uniquely identifiable persons or vehicles is not made practically feasible. By this we mean that the information collecting and/or verifying authority in general does not need to obtain access, or reasonably cannot even obtain access, to information – considered to be privacy-sensitive – on the movement patterns of a certain vehicle or person of which the identity can be tracked.

---

[17] And that is here the essential point.

[18] The essential point is that there are two measuring points of interest.

[19] The essential point is that the complete 'behavior', in so far as relevant, is charged and that thus measurements must be performed continuously or very frequently. Thus, a – very – large or – almost – boundless number of measuring points are of importance.

- 8 SEP 2003

The last part of the previous sentence is of importance, because tracing of permanently anonymous, i.e. not identifiable, vehicles and/or persons presents no danger to the privacy. This formulation does not only cover the situation that the identity can be determined via the traffic information system, but also the situation that the identity – immediately or later – can be tracked in another way. Notice that unlimited, complete tracing of an as yet not identifiable person or vehicle presents a considerable danger, because there is then a real chance of later identification. The privacy threat resulting from an as yet anonymous tracing will become smaller as the maximum duration and/or distance to which such a tracing is limited, becomes smaller. If there is a sufficient restriction on the said duration and distance, then there is no real danger for the privacy or, more precisely, the privacy risk may be considered to be acceptable.

In such a case we speak of legitimate tracing. It should be clear that this is fully justified by looking at the current practice. After all, when any citizen sees a car pass by (i.e. does trace that vehicle for a rather limited time and distance) and next determines the identity of that vehicle – usually correctly – by reading the license plate, it is generally accepted that this is in no way an illegitimate tracing.

The addition of the word 'illegitimate' in the formulation of the property mentioned has a second reason also. Often one wants to prevent that tracing can occur unrestrictedly, while at the same time one does really want tracing to become possible in certain – preferably in law embedded – circumstances and under certain – preferably in law embedded – conditions. On the one hand, think for example of trajectory speed checks, in which the average speed of a vehicle over a certain trajectory of, say, several kilometers is determined by identifying a person or vehicle both at the beginning and at the end of that trajectory, and by determining the elapsed time between both identifications. In this example, the length of the traveled trajectory is usually rather limited, so that this example perhaps is not sufficiently convincing. Therefore, on the other hand, think for example also of the possible tracking stolen vehicles or even the possible tracing of major criminals.

In Chapter 15 we will show that, by means of semi-identifications, vehicles can be traced well enough to make it possible, for example, to perform trajectory speed checks or even to measure traffic congestion delays without really endangering privacy. These forms of tracing we would therefore like to entitle as legitimate. (Let it be clear, first, that this concerns a weighing between the practical usefulness and the risk, and second, that we consider the risk to be sufficiently small to justify turning the scale in favor of the practical usefulness. One can judge for oneself how small this risk is after reading Chapter 15.)

In closing, we here superfluously repeat the remarks given earlier in a footnote regarding our use of various formulations. In this text, 'privacy protection with respect to movement patterns' and 'hindering illegitimate tracing' mean the same. For convenience, the addition of 'with respect to movement patterns' will often, and the addition 'illegitimate' will sometimes, be omitted. We also often speak briefly of 'prevention' or 'hindering' instead of 'not making practically feasible.' What exactly is meant will generally become apparent from the context. The cumbersome formulation 'not making practically feasible' has been mentioned earlier – and is mentioned here again – because of its greater accuracy compared to 'prevention.' After all, as is apparent from the above given examples, tracing is already possible to a certain extent anyway, and a traffic information system, of course, cannot prevent such tracing 'behind its back'.

-8 SEP 2003

4 Fraud resistance

Strictly speaking, one can only speak of – absolute – fraud resistance if no kind of fraud at all is possible. In practice, one often already speaks of – sufficient – *fraud resistance* if there is resistance to every known, practically feasible and profitable form of fraud against which the interested party wishes to protect itself. After all, it is in general difficult to protect oneself against all as yet unknown forms of fraud. And sometimes one does not wish to protect oneself against certain known forms of fraud, because the risk of unacceptable damage is reckoned to be too small (whether in proportion to the costs of protecting against it or not).

We use the term particularly in the second meaning. In this text the interested party, i.e. the one who wishes to protect himself against fraud, is mostly the authority, and we therefore generally view fraud resistance from the viewpoint of the defense of the interests of the traffic information system and the authority respectively. Said interest includes particularly the correctness of certain information that is collected. By means of checks on the reliability of that information we can provide for – at least a part of the – fraud resistance.

With the above, we think we have made sufficiently clear what *fraud resistance* means. In particular, it should now be sufficiently clear what we mean by a fraud-resistant traffic information system[20]. However, it seems useful to digress somewhat further on the application of the term to an individual component. We make an attempt to create extra clarity by giving below a supplementary, more detailed and informative description of the concept of fraud resistance applied to an individual component.

In this text, an individual *component* (in a vehicle) is in general called *fraud-resistant* if that component is inherently (!) protected in such a way that it cannot reasonably be forged, i.e. if it is in itself protected in such a way that it does not pay or is not practically feasible to forge that component. With forging is not only meant the making of a – deceptive – imitation, but also the manipulation of that component (at the expense of the authority as interested party). With respect to this last point think, for example, of – for the authority – negatively influencing the functioning of the component (excluding destruction) or pilfering crucial information (such as, for example, a cryptographic key) from the component.

For example, a magnetic card is thus not fraud-resistant, not even when the information stored in it is protected by cryptographic techniques. After all, making an imitation in the case of a magnetic card is relatively easy, since the bit patterns on a magnetic card can be read without too many problems. Furthermore, it is true that a magnetic card is not protected in itself against manipulation, because reading, writing and/or changing its bit pattern is rather simple. Thus, it does not matter that the total system (that makes use of the magnetic cards in question) might indeed protect itself with the use of cryptographic techniques against certain forms of fraud with magnetic cards, such as, for example, against comprehensive reading or meaningfully changing the bit pattern on it. For other passive means for data storage, something similar applies of course.

Note that with certain electromagnetic devices or aids, such as, for example, magnetic and chip cards, there can generally only be an imitation if one manages to copy or produce certain crucial bit patterns (that for example are a representation of software or data, which particularly also include cryptographic keys). To be able to copy or produce such crucial bit patterns, it is usually necessary to worm these or other crucial bit patterns out of one or

---

[20] We concentrate our attention (almost self-evidently) on the fraud resistance of components in the vehicle and of the communication via transmitters.

-8 SEP 2003

more authentic specimens first. But then there is first a question of manipulation of an authentic specimen at the expense of the authority. In short, manipulation at the expense of the interested party is generally the dominant form of forgery with electromagnetic means in general.

Note also that with the fraud resistance of an individual component, the physical protection in general plays a dominant role and is the decisive factor. On the other hand, in a larger whole, like the total traffic information system, logical protection measures (such as, for example, the application of cryptography, inspections and organizational measures) do play a major role. When evaluating individual components for their own fraud resistance, the logical protection in the larger context does not count. This in a way adds to the dominant role that physical protection plays in the case of considering individual components.

Further we like to elucidate somewhat that the choice of the viewpoint, i.e. choosing the interested person or party, plays a role. Suppose that users of a certain system have to identify themselves by placing digital signatures, and that they use some aid or aids, for example in the form of magnetic or chip cards, when doing so. (See also the Chapters 6 and 14.) From the viewpoint of each owner of an identification aid, his own identification aid then must preferably be fraud-resistant to prevent someone else from being able to take advantage of his digital signature in any way. But from the viewpoint of the authority (of the system), the identification aids do not need to be fraud-resistant at all, since in principle every correct signature can be accepted. The way by which the signature has been created (whether or not by using an aid, authentic or false), does play no role in the validity of digital signatures.

There is yet another, at least as important aspect (concerning the choice of the viewpoint) that deserves attention. Suppose that the identification aid is not protected against, for example, manipulation or copying. From the viewpoint of the owner the aid is then not fraud-resistant, since his interests can be damaged (particularly by copying). The owner will then have to be really careful with it. In our example, it is solely the responsibility of the owner to prevent abuse of his identification aid and the interests of the authority are not impaired by forgeries. Thus, from the viewpoint of the authority, the said identification aid is in a certain sense 'fraud-resistant', because no fraud at the expense of the authority can be committed with it. (At least not directly at the expense of the authority, although perhaps indirectly. See also the end of this section.)

In general, a component for which the fraud resistance is irrelevant, will not be called fraud-resistant. In the description given above, our addition of 'inherently', and of 'in itself' respectively, plays a role in this regard. Despite all the effort that we have taken to find a formulation that is as close as possible, our formulation is probably not completely waterproof either. Finding a waterproof formulation is usually at least difficult or even impossible. But with the given elucidation, one thing and another is deemed to be sufficiently clear. (Of course this remark is not only valid for the, in our case, important notion of fraud resistance, but also for all other notions that we use and that are of importance, such as in particular tracing, agent, semi-identification, and the like.)

Finally, we make two more remarks on the example above. In the example above, it may seem that only the card holder in question and the authority could be regarded as interested parties. That possible impression is incorrect. All other card holders are, to a certain extent, interested parties as well. For, all card holders have an interest in the fact that another person's authentic card cannot be manipulated (i.e. forged) in such a way that their own digital signature can be put with it. So, fraud resistance from the viewpoint of other card holders can also be of importance.

-8 SEP 2003

Besides, it can be, and usually also will be, the case that the authority, even if a different authority is responsible for the identification aids in question, does really have an – indirect – interest in the fact that card holders cannot cheat each other too easily. After all, this might result in the users turning away, or wanting to turn away, from the authority's system, i.e. not wanting or no longer wanting to use it.

5 Equipment

5.1 Overview of the tasks of the vehicle equipment

In first instance we will restrict ourselves – for a moment – to tasks related to traffic pricing. We assume that in each participating vehicle equipment [alternative translation: apparatus] will be present during participation in traffic to perform the required tasks. This *vehicle equipment* (VE) will in case of the TIP system then often perform the following tasks: 1) retaining, measuring and/or reading certain data that are required for the working of the TIP-variation in question and that are related the vehicle, its movement, fuel consumption, exhaust gases or the like, 2) keeping one or more counters up-to-date according to a prescribed algorithm and on the basis of the required data, 3) transmitting certain prescribed data, such as, for example, speed or counter value, which are necessary for the traffic pricing and/or the verification of the correct functioning. If the vehicle equipment includes a receiver, in general also: 4) reacting adequately to requests or commands that are received from the authority, i.e. from authorized organizations.

5.2 Required vehicle equipment

For a TIP system, certain equipment must be present in each participating vehicle. Usually only part of the means and/or elements mentioned below are necessary.

1) A small number of processors with associated memory, among which also a quantity of non-volatile memory (i.e. memory that is protected against power failures, or memory of which the contents anyhow remain unimpaired in the event of a power failure) for preserving essential software and data, such as, for example, algorithm(s) for derived information, counter values and/or cryptographic key(s).
2) A transmitter and/or a receiver for communication with the outside world (and a connection to it).
3) A number of sensors and/or measuring instruments in the vehicle – and connections to said sensors and instruments – to be able to ascertain or read out all sorts of data, such as, for example, the engine speed and/or the kilometer counter value.
4) Other equipment in the vehicle with which communication and/or cooperation can take place, such as, for example, a cruise control (and connections to said equipment).
5) Equipment for communication with users, such as, for example, a display and/or a speaker for supplying information to users of the vehicle and, for example, a microphone for receiving information from users (voice-input), and connections to said equipment.
6) A number of – preferably standardized – connection points, such as, for example, magnetic or chip card readers, for making a connection to loose equipment yet to be connected, such as, for example, a consumption pass and/or user card to be applied by or on behalf of the payer, which, for example, encompass a counter value and/or an identification device.

-8 SEP 2003

7) A – preferably standardized and central – connection point for making a correct mutual connection between all equipment[21].

Figure 1 gives a schematic illustration of a possible situation. In which cases the above-mentioned equipment components must, may or have to be present or not, and for what purpose(s) they can be used for example, will become clearer bit by bit in the course of the further explanation. Below we already offer some elucidation. All equipment mentioned is obtainable and/or known in various forms in the prior art, and therefore we will not digress on the equipment itself. However, if in certain cases or for certain reasons special demands are, or must be, made from the components, we will – try to – mention that explicitly.

In our further explanation of the TIP system, we assume that all processing is performed by maximally three processors, although the work also can be distributed, of course, over more processors. Also processors that are present in other mentioned components, may be used. The fact that we do mention explicitly the possibility of two or three processors, only has to do with possibly wanting to keep strictly separated on the one hand the possible processing on behalf of 1) the authority (i.e. the processing for exercising supervision by a possibly present agent), and, on the other, the processing on behalf of 2) the holder of the vehicle and/or 3) the user or the payer. (The latter two processors serve, for example, for putting digital signatures and/or for exercising supervision on the agent on behalf of the holder and of the user or payer respectively.)

A reasonable possibility is, for example: 1) a fraud-resistant processor, attached to the vehicle or not, that acts as agent, 2) a processor, fraud-resistant or not, attached to the vehicle for supervision on behalf of the holder of the vehicle, and 3) a processor on a chipcard either of the vehicle's user himself or of the *payer*, i.e. of the person or organization that accepts the responsibility for the use of the vehicle and thus in particular also for the payment of the charges due to the use of the vehicle[22]. (Think, for example, of traffic pricing and traffic fines.) This third processor is not rendered in the example of Figure 1, but the chipcard reader required thereto is (see below).

In Figure 1, a bold-printed frame indicates that the component in question is fraud-resistant or that the authority must trust on sufficient fraud resistance of that component. If no agent is used, then the left processor in Figure 1 will be dropped. If an agent is used and joint use of one processor is acceptable to both parties (for example, because there is a manufacturer of fraud-resistant processors that is sufficiently trusted by both parties), then the

---

[21] This connection point will possibly also be used for the connection of – at least a part of – the equipment to a power supply. As the need for a power supply is self-evident, we have not mentioned a whether or not central power supply, such as, for example, the battery of the vehicle or separate batteries, when enumerating the possibly required vehicle equipment. Also in the following we will pay – almost – no attention to this rather obvious aspect.

[22] Precisely because of this possibility we have, earlier in this text, already taken this distinction between user and payer into account a number of times. In the further text we will often choose, or try to choose, for the most appropriate term in the context concerned. That does not alter the fact that both the word 'user' and the word 'payer' sometimes can stand for 'payer and/or user. Note also that the user does not necessarily have to be the driver. Thus, there can be a – perhaps somewhat subtle – distinction between driver, user and payer. As the context generally gives sufficient grip, we do not have to be always that precise with our use of words in this text.

right processor of Figure 1 may be dropped. We here already emphasize that it is very well possible to use only one processor per vehicle instead of two or three (or possibly even more).

By the way, it is even possible that there is no – question of a – 'real' processor in a strict sense at all. If, for example, only the vehicle registration number and/or the kilometer counter value of the vehicle, or a certain part of said value, is transmitted continuously, then there is no or hardly any question of 'real' processing exclusively for the benefit of the TIP system. It may be clear that in this latter case also most of the other components or kinds of components rendered in Figure 1 will be dropped.

For the non-volatile memory used, it is in general true that – only – a small amount of it is required to be writeable as well as readable.

Often the said sensors and/or measuring instruments will already be present in the vehicle, and only adequate connections to that equipment still require implementation, if desired at all. Think, for example, of connections to sensors already present on the crankshaft and drive shaft, or – instead – to a possibly present electronic revolution counter and kilometer counter. But of course one can also introduce equipment especially for use by the TIP system. In Figure 1, only one sensor or measuring instrument, say the kilometer counter, together with its corresponding connection is explicitly rendered.

The category connections to other equipment in the vehicle could in principle also be considered to include the possible connection or connections to separate equipment for fraud-resistant identification and/or for fraud-resistantly preserving of and giving access to data concerning the classification of the vehicle, such as, for example, year of make, brand, model, gearbox type and engine type. This is also true for a possible connection to separate equipment for keeping track of the time (i.e. a clock) and for placing digital signatures on behalf of the vehicle or the holder of the vehicle. Later we will return extensively to the subjects identification, classification and digital signatures. We will then show, among other things, that digital signatures can be used for excellent fraud resistance of identification and classification.

However, if – or in so far as – the tasks mentioned in the previous paragraph require processing, we assume for convenience that such functions belong to – or are combined with – the tasks of one of the above-mentioned processors. This assumption does not lead to an essential restriction of the generality of our explanation, but does help to keep Figure 1 simple and to avoid that we would – have to – enter into all kinds of details or difficulties pertaining to security aspects which are not specific for our invention and on which we here do not want to digress further. The other equipment – and the connection to other equipment – rendered in Figure 1 may concern, for example, the cruise control of the vehicle.

The transmitter or the receiver is not strictly necessary for all variations of the TIP system, but is usually at least handy. One thing and another will later become clearer of itself. In Figure 1 there is – a question of – a combined transmitter plus receiver.

Application of voice-input is perhaps an aspect for the somewhat longer term, although the technique in this area has already been advanced substantially. In Figure 1, only one component for communication with a user, say a display, has been rendered explicitly. It may be expected that for output usually at least a speaker will be present as well.

In relation to the connection points for the benefit of equipment to be connected, we remark that a – at least in the case of certain variations of the TIP-system – supervising agent may be implemented on a detachable chipcard.

-8 SEP 2003

(Later we will show also that such an agent that has been realized as loose vehicle equipment, may also take on the task of consumption pass.) Also, the processor that performs certain tasks on behalf of a user or payer, such as, for example, placing digital signatures and/or supervising the possible agent, may be implemented on a loose chipcard. In short, both processors just mentioned thus may be connected to other equipment by means of a chip-*card reader*[23]. It is quite plausible that at least the possible processor of – the holder of – the vehicle will be attached to the vehicle. In Figure 1, the two processors for the agent and for – the holder of – the vehicle respectively, are mutually connected via the central connection point, and the card reader is intended for a user card.

A *user card* is – primarily – an aid to be able to ascertain which person or organization accepts the responsibility for – the costs of – the use of a vehicle. Thus, it may primarily be a device or aid for the identification of the payer. A *consumption pass* has – primarily – the task of keeping record of a counter value for the benefit of the user and possibly also for the benefit of the traffic information system. The counter value may, for example, concern the use by a certain person, such use possibly being distributed over several vehicles and such use being for one's own account or for the account of a certain organization, such as, for example, the employer. If the kept counter value is of essential interest for the traffic information system, then consequently the consumption pass will form part of the traffic information system. If, to protect the counter value or values, the consumption pass must, from the traffic information system's or the authority's point of view, be fraud-resistant, then the consumption pass is an agent as well. (Note: The counter values stored in or on not fraud-resistant means, such as, for example, magnetic cards, can also be protected in another way against certain kinds of abuse.)

The above descriptions make it possible, in principle, to clearly distinguish between user cards and consumption passes. However, for convenience and because both functions may also occur combined on one card, we will henceforth often use the term *user card* for both notions. Later we will return to the case that the user card contains, or contains also, an agent, or is itself an agent as well. (Or, in yet other words, the case that the agent takes on the tasks of user card as well.) At the risk of laboring the obvious, we here remark yet that, if for the use of a vehicle a user card and/or an agent on a loose chipcard is required, then the user of the vehicle has to 'offer' such a card, i.e. must connect that card or those cards to the other vehicle equipment. (For example, by putting it into the slot of a card reader.)

A central connection point is not necessary at all. The connection of all equipment can also occur in many other ways. However, a central connection point does lead to a simplification of the physical organization of the equipment and of our rendering of an example thereof in Figure 1.

A disadvantage of Figure 1 is that it seems as if both processors have equal access to all other components. However, that definitely does not have to be so. It is, for example, well-imaginable that only a processor of the holder or of the payer has direct access to the transmitter and receiver in the vehicle, and that the processor on behalf of the authority, i.e. the agent, certainly does not. Then the agent thus cannot freely and without limitation send all kinds of – secret – messages to the authority, but has to do so via another processor that thus can keep an eye on – the communication by – the agent.

---

[23] Despite the misleading name we generally assume that a card reader enables communication in both directions, i.e. also enables 'writing'.

-8 SEP 2003

In Figure 2, we have rendered the situation of Figure 1 in a slightly different way in order to make such an aspect of the 'logical' organization of the equipment stand out better[24]. Thus, even when the physical connections are realized as suggested in Figure 1, the logical organization still can be as suggested in Figure 2. Figure 2 is intended to express that the rendered processors can communicate with each other and both have direct access to all other equipment with the exception of the transmitter and the receiver. In this example, the processor on behalf of the authority, i.e. the agent, can only obtain access to the transmitter and the receiver with the assistance of the other processor, i.e. can only obtain indirect access to the transmitter and the receiver.

5.3 Protection against fraud

When using the traffic information system for traffic pricing, for example, the need for sufficient protection against fraud is self-evident. Therefore, it seems plausible that – at least a part of – the equipment used by the traffic information system, in a vehicle must be fraud-resistant itself and perhaps must also be attached to one specific vehicle in a fraud-resistant way, so that it is warranted that certain parts cannot be removed for – illegal – use with another vehicle.

How in case of TIP systems one can ensure a good or even excellent resistance against – attempts to – fraud, will be made clear in the course of the further explanation. Here we already remark that, in the case of the TIP system, the protection of equipment in vehicles is relatively easy and inexpensive, since the physical protection generally can be restricted to the agents used, if any. In case of a TIP system without agents, the equipment involved in each vehicle thus does not have to be physically protected at all! Also, in the case of a TIP system with agents, the physical protection will not be expensive at all, as chips can be physically protected at low costs and because for each agent one chip with corresponding software suffices. Furthermore, the number of agents in each vehicle can be restricted to one.

In certain cases, an agent additionally must be linked in a fraud-resistant way to one specific vehicle. This is the case, for example, if an agent is used, or also used, for fraud-resistant identification and/or classification of the vehicle, and if a very high level of fraud resistance is required. Often other measures, such as simple and early detection of removal or destruction, can suffice. We will return to this later. (See Chapters 14 and 17)

If, nevertheless, one considers it wise to give the other vehicle equipment – also – some physical protection in order to discourage attempts to commit fraud, one can confine oneself to very cheap measures, because that extra security is not of essential importance, i.e. does not need to offer full protection.

5.4 Minimizing the use of physical protection

With security, there is always a question of some kind of arms race. Particularly with physical protection, one can find for each protection measure one way or another to get around that measure, which makes further protection measures necessary, which invites new counter measures, etc., etc. A high level of physical protection therefore generally goes hand in hand with high costs. This is the more so because of the necessity of carrying out physical inspections regularly, which is laborious and expensive because of the personnel costs for the inspectors. This all

---

[24] The fact that in both figures the connections cannot only be interpreted as physical connections, but also as connections of communication, was an extra reason for us to omit – the physical connection to – the power supply or supplies from the figures.

-8 SEP 2003

explains why, in general, we would rather not have the fraud resistance of a system depend on all kinds of physical protection measures.

With the TIP systems to be described by us, a very high level of security and also of privacy protection can be achieved. For this, one can, as we will outline, make use of organizational measures and, in particular, also of cryptography[25]. When using cryptographic techniques, it is true that there is also an arms race, but in this case the security level generally can be increased easily by starting to use larger numbers, i.e. larger bit patterns. The increasing computing power due to the ongoing development of faster and faster chips forms no real threat to the security of cryptographic techniques. It is true that the increased computing power makes deciphering increasingly easier, but that applies to enciphering as well. In the case of cryptographic techniques, the security is rather based on an essential difference in complexity between certain operations on numbers. Thus, a very high security level can remain being guaranteed, as long as there remains a substantial difference in complexity between the underlying computations.

Because the security level, when using cryptographic techniques, depends on, among other things, the degree to which the cryptographic keys used are secured, in general some kind of physical protection will really come into play when using cryptography. If, for example, the keys used are being stored in chips, one also needs some form of physical protection for securing these chips against extraction of their contents. However, this form of physical protection, which is used with chip cards amongst other things, has proven in practice to be able to offer a high level of security at low costs, so that we do not consider its use difficult to accept. Even better, we see it as an advantage of the systems developed by us that the physical protection (of the vehicle equipment in particular) can be restricted to this specific, cheap form, of which the reliability has proven itself.

5.5 Equipment already present

It is to be expected that within the foreseeable future most of the above-mentioned equipment will be standard equipment for new cars. This equipment can, or will be able to, carry out a multitude of tasks, such as, for example, supervising the correct functioning of – parts of – the vehicle, keeping accounts for the benefit of automated diagnostics (possibly remotely), supporting navigation, sufficiently fraud-resistant retaining of, and granting access to, an identification number of the vehicle for service and guarantee purposes, remembering the desired settings of, for example, steering wheel, driver's seat and mirrors for various drivers, simplifying tracing after theft, implementing a tachograph or black box, communicating with parking machines to automatically establish parking fees and possibly also for direct or indirect automatic payment of parking fees, communicating with all sorts of other provisions alongside the road, with other vehicles and/or with the rest of the outside world, etc., etc.

Thus, in the future only a fraction of the mentioned equipment will, or will have to, be present exclusively for imposing traffic fees with the assistance of the TIP system. After all, only the non-volatile memory word(s) for the counter value(s) or the traffic fee counter value(s) seem to be intended exclusively for that purpose. All other parts may also be useful and/or necessary for other tasks.

For example, the connection point for, for example, a chipcard may already be present – or also going to be used – for tasks, such as, for example, determining by or on behalf of whom the vehicle is going to be used in order to

---

[25] Actually cryptology. See also the chapter on cryptography.

-8 SEP 2003

be able to determine whether that use will be permitted and/or in order to automatically adjust the driver's seat, steering wheel, mirrors, and the like according to the wishes of the user registered in a chip card. The receiver can be used, among other things, to take delivery of data about the infrastructure, such as, for example, the locally valid speed limit or information on delays as a result of tailbacks. In short, there are numerous other useful applications possible, even too many to mention.

5.6 Possible integration with other applications

Because the equipment used in vehicles by – the traffic fees part of – the TIP system does not or hardly need physical protection to hinder fraud, the traffic fees part can easily be integrated or cooperate with all kinds of other applications. If desired, certain other applications can therefore also form, or start to form, part of the total TIP system. The equipment required for the traffic fee part of the TIP system, or for the total TIP system, thus may be used collectively with other applications within or outside the total TIP system, so that the costs that will have to be made per vehicle for – the traffic fees part of – the TIP system, may be low or extremely low.

5.7 Fixed and loose vehicle equipment (FVE and LVE)

Not all equipment mentioned needs to be, or needs to have been, permanently attached to the vehicle. The equipment or important parts thereof may be loose[26] and may, in the case that there is a connection point, be connected to fixed vehicle equipment, such as, for example, sensors and/or the battery. The loose, connectable equipment may, for example, consist of a chip card, which can take care of a part of, or even all, processing and/or which contains – at least a part of – the non-volatile memory. It is also possible, for example, that the transmitter and/or the receiver form part of the loose equipment.

With the term fixed vehicle equipment (FVE) we henceforth will allude to all equipment that is permanently attached to the vehicle and that supplies information to, or is used – directly or indirectly – by, the TIP system. And with the term loose vehicle equipment (LVE), we will allude to all other equipment that during participation in traffic is present (and possibly connected to the FVE) in the vehicle for the benefit of the TIP system. We will keep on using the term vehicle equipment (VE) for the union of FVE and LVE.

On the one hand it is possible that there is only a question of FVE, i.e. that all equipment is permanently attached to the vehicle and that no use is being made of loose, connectable equipment. On the other hand it is possible in certain cases that there is only a question of LVE. The latter is only possible if no use is being made, or made yet, of sensors attached to the vehicle (for example, to be able to determine the kilometer counter value) or of identification means that have been fraud-resistantly attached to the vehicle, such as, for example, a chip with an identification number and/or a type indication. Because otherwise there also would be a question of FVE. It is self-evident that there is a whole range of other possibilities between both extremes.

Normally a TIP system that is used for traffic fees and particularly for traffic pricing will also support continuous pricing, for which it is in general necessary to make use of data that are acquired via sensors on the vehicle con-

---

[26] We are aware that in general there is no clear distinction between what can be called 'loose' and what can be called 'fixed'. For example, the battery of a vehicle is in a certain sense also fairly easily detachable, so that against our intention it might be considered also as a loose part of the vehicle. However, a more precise definition does not seem necessary for our purpose.

-8 SEP 2003

cerned. Thus, in general there will be a question of FVE, to which LVE can be connected or not. However, when introducing road traffic pricing with the assistance of the TIP system, one can also restrict oneself – possibly only in first instance – to open and closed tolling. (See also Chapter 17.) In doing so, one then may limit oneself, for example, to transmitting an identification number of the payer or of his checking account. Thus, data concerning the vehicle then are not necessary, so in this case having only LVE can suffice.

5.8 Broad interpretation of the notions used

Perhaps superfluously but to be quite on the safe side, we remark explicitly that, in general, the notions used must be interpreted broadly. Not only the notions dealt with in this chapter, but all notions in the entire text. For example, we will use the concept of transmitter for every means by which a message can be given or made available to the receiver(s) of other objects or persons in the environment. The term is usually used if there is no question of physical contact and messages are being transmitted by means of, for example, sound or radio waves, light, infrared, or whatever[27]. But in our context, the term obviously also covers those cases in which the transfer of messages occurs via physical contact, for example by means of electrical conduction. Thus we could also have entitled the possibly present connection point for the connecting of equipment of, or on behalf of, the payer as a transceiver. This last remark illustrates that the earlier-used term connection point, without it being said explicitly, really was intended to be interpreted broadly, so that it also includes cases without physical contact. In short, the communication between LVE and FVE can also take place via transmitting and receiving means.

6 Cryptography[28]

In general, the suggested TIP systems gratefully use prior art cryptographic techniques for various purposes.

By means of cryptographic techniques it is, for example, possible to keep the contents of a message secret for any other person than the intended recipient. In the following, we will refer to a message as *secret* if that message has been enciphered in such a way that only the intended recipient can decipher it or, in other words, can undo the message of the 'packing' that provides for its secrecy. This situation is somewhat comparable to a sealed envelope around a letter, albeit with the difference that anybody can indeed illegally open a sealed envelope, but not a secret message. (The comparison with a sealed envelope is not unusual, even though a safe vault of which only the sender and recipient have a key, offers more similarities in properties.)

Furthermore, by means of cryptographic techniques it is possible to warrant the authenticity of the contents and/or of the sender of a message. If both aspects are guaranteed, one speaks of a digital signature on that message. Henceforth we will refer to a message furnished with a digital signature as a *signed* message.

To hinder fraud, each message should not only be signed, but also provisions should be taken to ensure that only the copy of each signed message that is received first really counts, i.e. that all copies that – possibly – turn up later anywhere cannot get any effect in addition to the – intended – effect of the copy received first. To this end,

---

[27] A display and a loudspeaker thus also fall under the broad notion of transmitter.

[28] More strictly speaking, 'cryptography' only stands for ciphering. The correct term for the theory of both enciphering and deciphering (say, both producing and reading ciphertext) is actually 'cryptology'. In the rest of this text we will nevertheless continue using the somewhat more well-known and quite current term 'cryptography'.

-8 SEP 2003

the original copy of each signed message should be at least unique. Usually the desired uniqueness is obtained by adding a timestamp or a serial number to each message. Furthermore, to this end the intended effect of each message should be clear. The intended effect is often made clear by recording in each message explicitly, among other things, the addressee and/or the subject. Besides that, for a good signature, it is generally necessary to also incorporate into the message a known bit pattern (or a bit pattern that is derivable from the rest of the message).

We will not digress further on these kinds of cryptographic details, and henceforward will pay no – or hardly any – attention to them. To put it even stronger, we will – perhaps – sometimes not even indicate explicitly whether secrecy and/or signing is either desirable or necessary for a proper functioning of the various protocols that will pass in review. A person skilled in the art should himself be able to determine, or further determine, which protective measure(s) are necessary and how these can be implemented by means of cryptographic techniques.

Nevertheless, we will pay quite some attention to a number of security aspects. Not only to show here and there what application of cryptography has to offer, but also to make the explanation of a number of aspects of the protocols and of the working of TIP systems clear or more clear. Thereby we will – try to – restrict ourselves to the two properties *secret* and *signed*. Thus, in our description, the stronger means of digital signatures is sometimes mentioned, while it might suffice, for example, to warrant the authenticity of only the sender or of only the contents of the message. Also, we will indicate here and there that secrecy or signing takes place or should take place, while one may also content oneself with a similar approach without these cryptographic additions. In short, the descriptions given serve only as illustrations and may not be understood as imposed restrictions.

7 Accounting

7.1 Data to be maintained

As mentioned earlier, we will initially focus on imposing traffic fees. The data that needs to be actively maintained [alternative translation: recorded and updated] by the vehicle equipment will then in general include anything that affects – the level of – those fees (say, is used as a parameter). These data can be of any kind. For example, in a vehicle with a combustion engine one could, at least in principle, continuously measure and record the quantity and quality (kind) of the exhaust-fumes produced by said vehicle. However, in most cases it concerns data that can be determined more cheaply, such as, for example, the distance covered, the speed, the point in time, number of revolutions per minute, vehicle type, engine type, the gear engaged, the position of the gas pedal, etc.

7.2 The kilometer counter as odometer

Below we will give a number of examples in which a record is kept of at least the kilometer counter value. Strictly speaking, instead of kilometer counter we perhaps should start to use the uncommon [Translator's Note: uncommon in Dutch] word odometer, because – in the case of the kilometer counter as intended by us – the distance unit (or the smallest distance unit) used for the counting can be – and because of the desired accuracy in general also will be – different from the kilometer. Nevertheless, we will continue to use the common [Translator's Note: common in Dutch] term kilometer counter for the odometer all the time. In the rest of this text we assume that the kilometer counter is kept up-to-date, and can be read, in a sufficient number of decimals.

-8 SEP 2003

7.3 Some examples

As an illustration, we will give some specific examples. In the first example, only the kilometer counter value is recorded (to a sufficient degree of accuracy). In this case the corresponding traffic fee may consist of a fixed price per distance unit traveled.

In the second example the kilometer counter value is recorded, as well as the time, speed, and accumulated fees paid and/or due. Each of these four values must, of course, be expressed using some prescribed unit. For example, the fees due can be expressed as a sum of money, or in terms of 'levy points', etc. The way in which dues are calculated from the other data, will of course be prescribed (presumably by government).

Continuing the second example, the prescribed amount that must be contributed to the accumulated 'levy points' for each distance unit traveled thus may depend on the time span (i.e. the speed) in which the distance was covered, and on the precise period (i.e. date and time) in which it was covered. To put it another way, in the given example the price due for a unit of distance traveled can be determined by any desired function of speed and time. For example, it is possible for kilometers traveled at a speed higher than, say, 90 km/h to be charged at a progressively higher rate (i.e. the charge per kilometer increases with speed). The same applies to kilometers traveled during specific peak hours on specific days. Another possibility is to follow a U-shaped function of speed, and thus additionally increase the charge per kilometer as the speed drops further below, say, 60 km/h. The reasoning behind such a U-shaped function is that the fuel consumption and/or the pollution caused per distance unit is greater at both high and very low speeds.

Our third example augments the data used by the second example with the license plate number (or some other registration number) of the vehicle. The license plate number register (to be) maintained by, or on behalf of, the government might, for instance, include an accurate description of the vehicle type, engine type, etc. of the vehicle concerned. Therefore, for any vehicle type, i.e. for any combination of brand, model, year of manufacture, gearbox and engine type (etc.), one now can choose the price function in such a way that the price per distance unit traveled will be fairly accurately related to the fuel consumption and/or environmental pollution caused, without having to continuously measure and/or analyze the exhaust fumes of each individual vehicle. Note that one can choose to let the price per kilometer depend not only on the average speed at which this distance unit was traveled, but also on the average speed at which the preceding distance unit was traveled. Therefore, additional pollution (and/or fuel consumption) resulting from speed variance, i.e. acceleration and deceleration, can be charged fairly accurately without having to continuously analyze exhaust fumes emitted by the vehicle while participating in traffic.

7.4 Empirical discovery of an algorithm

In order to arrive at a sufficiently accurate algorithm for calculating the degree of pollution caused by a vehicle from relevant data (such as speed, acceleration, temperature, fuel consumption, engine speed, etc.), one would like to perform actual analyses and measurements on at least one specimen of every possible kind of vehicle. The kind and quantity of environmental pollution caused by the specimen under all kinds of conditions should be analyzed and measured, and the corresponding combination of relevant data determined. One specimen may be sufficient already, since we can collect data of all other vehicles of that type through the traffic information system, and check whether they manifest the same characteristic combinations of data relevant to this calculation. Another use of the data thus obtained is to call in for closer inspection those vehicles that seem to deviate. Simi-

-8 SEP 2003

larly, one can track down vehicles that no longer conform to – environmental – standards, perhaps due to bad tuning or aging. (Observations similar to those described here apply to the example of overall noise production by a vehicle. This latter example of using derived, i.e. calculated, information is addressed in Chapter 11.)

If one decides to base the fee on fuel consumption, often even no specimen at all is necessary for prior experimentation. The reason is that one can collect, for every type of vehicle, all information on (reported) fuel consumption under all kinds of usage conditions through the traffic information system. After filtering out any results deviating too far (perhaps due to attempted fraud), accurate information on fuel consumption occurring in practice can be derived per vehicle type. The results thus obtained can be used to determine a sufficiently accurate algorithm (e.g. in the form of a function or a multi-dimensional table) for calculating the fuel consumption from a suitable (e.g. minimal) number of input parameters. Such an algorithm can subsequently be used to verify the fuel consumption reported by an individual vehicle. (Observations similar to those described here apply to the possible use of the traffic information system to collect measurements of the level of noise production occurring inside the engine compartment of vehicles).

Either of the two ways described above for empirically discovering an algorithm for calculating derived information may also be applied to data other than fuel consumption (or noise production). More in general, one can automatically collect the information required for combating fraud with a particular type of vehicle provided that the great majority of the vehicles of that type are not subject to fraud.

7.5 Some more examples

Another possibility is to let the pricing function used for a particular traffic fee vary with (depend on) the area or the section of road. Obviously, one must then keep track of the tariff zone in which the vehicle is located. For example[29], assuming the vehicle equipment includes a receiver, it can be kept informed about which tariff, i.e. which price function must be applied, by announcing via a transmitter at each border crossing between different tariff zones to the vehicle equipment the kind of tariff zone that is being entered. One could also let the fees due be dependent (wholly or in part) on the intensity of local traffic. Later, we will separately address a number of other advantages of the use of the receivers.

From the above it should have become clear that there are countless possibilities, too many in fact to mention. More or less as a coincidence, all of the examples that have just been given involve a kilometer counter. This is a coincidence in the sense that one can very well conceive situations in which the length of the distances traveled has no effect on – determining the level of – the fees. On the other hand, it is not a coincidence at all, since we expect that in practice a kilometer counter will actually be used in many cases eventually. After all, an important property of the TIP system is that it makes continuous pricing possible. This also explains why, in the remaining exposition, we will focus mainly on the use of counters. In our examples, we will often confine ourselves to mentioning counters (counters in general or kilometer counters in particular).

---

[29] The correct tariff can, for example, also be determined with the aid of a GPS and a description of the tariff zones/areas.

We point out in advance that all possible kinds of data of which either the reliability can be verified sufficiently easily from a distance, or which are sufficiently protected against fraud attempts in another way, can be used as parameters of the pricing function. We will return to this matter in Chapter 11.

7.6 A traffic fee counter value per person and/or per vehicle

All parameters that influence the level of a traffic fee are used in some prescribed way to maintain the current value of a traffic fee counter. In many cases this concerns a cumulative, in other words monotonically increasing, traffic fee counter. However, it may also concern a monotonically decreasing counter. To simplify our explanation, we will often refer to 'the counter', deliberately ignoring the possibility of maintaining more than one counter, and also leaving unstated what the one or more counters are associated with. For example, the traffic fee counter, i.e. the counter on which the payment process[30] is based, can be associated with a vehicle or with a payer. Another interesting alternative is to maintain two counters, one associated with the vehicle and one associated with the payer.

Associating a counter with the vehicle (and therefore indirectly with the holder of that vehicle) is a straightforward possibility, which closely matches the (ultimate) responsibility of the vehicle registration holder to pay the traffic fees that arise from the use of the vehicle. This possibility also closely matches the traditional association between kilometer counters and/or kilometer counter values, and vehicles.

The advantage of a direct association between counters and payers is that the users of a vehicle can alternate, and yet each of them will still be held accountable by the authority (in this case the fee collector) for payment of traffic fees arising from their own individual usage.

The possible charging of traffic fees incurred by a vehicle to its actual users can be considered to be the vehicle holder's own responsibility. If that is the case, the traffic fee counter is associated with the vehicle and it is up to the holder to keep track or have keep track of fees per individual user (possibly aided by LVE), if desired. Thus, in this case the holder will be responsible for the possible use of a second kind of counter.

Of course, it is also possible that the authority, i.e. the fee collector, is interested in both counters[31], and uses them both for the verification and/or payment process. Having a redundancy in the counters provides the authority with an additional means of verification (of consistency), since, for example, the total amount of traffic fees due according to the counters associated with vehicles should be equal to the total amount of traffic fees due according to the counters associated with payers.

In any case, for the sake of convenience, we will generally continue to speak of one counter in the remainder of the text.

8 Use of a transmitter

A realization of a TIP system in which no transmitter is used, seems unlikely. In the case of an approach using agents (which we will not discuss until in Chapter 16) it is, in principle, certainly possible to have the agents report, for example via an electrical contact, only during a periodic inspection. However, the use of transmitters

---

[30] For example, this might simply be a kilometer counter.

[31] For example, if individual pollution rights, tradeable or not, are involved.

- 8 SEP 2003

is so cheap and convenient that in the remainder we will assume the use of a transmitter. There is no reason to treat the 'more classical' possibilities without transmitter separately in more detail, since all relevant aspects are already contained in the remaining explanation of the case using a transmitter. (Note that communication by physical contact is also covered by our notion of a transmitter in a wide sense.)

8.1 Continuous or solicited transmission of data

If (or insofar as) the vehicle equipment in each participating vehicle keeps its own accounts, the authority must be able to gain access to the accounts of each participant at any desired moment in order to be able to perform effective supervision. In the approach with remote verifications only, which approach we will discuss first, every participating vehicle must for this purpose make crucial data available to the authority in the outside world via a transmitter. In Chapter 16, we will describe a similar approach in which these data are passed to an in-vehicle agent, i.e. a representative, of the authority. This agent then communicates via a transmitter with – the rest of – the said authority in the outside world.

The transmission of messages with the required data can take place – almost – continuously, that is to say the messages must be transmitted at least at a prescribed high rate, or else it can take place solely in response to an authorized request (or rather, to an authorized order). If one chooses for gaining access to the data kept in the vehicle upon request only, good verification from a distance becomes more difficult and therefore more expensive to perform, so that an adapted approach, such as the approach with agents residing in the vehicle, seems at least desirable. Until the treatment of the approach using agents in Chapter 16, we will – to the extent possible – confine ourselves in our remaining exposition to the case in which the required information is made available almost continuously via the transmitter.

8.2 Reading from a distance

The messages transmitted by vehicles (or more precisely, by vehicle equipment) can be read by means of receivers, without traffic being disturbed in any way. In principle, receivers can be placed at any desired distance, as long as they are within the prescribed range of the transmitters of the vehicles to be 'read out'. The necessary receivers may be placed, for example, alongside or above the road, but no other possibility is ruled out at all!

8.3 Possibly transmitting only identifications or semi-identifications

If the TIP system is used only, for example, to collect traffic information in a narrow sense, thus among other things to measure the quantity and/or average speed of certain traffic flows and/or to determine traffic congestion delays and/or to determine the (average) speed of individual vehicles on particular road segments, then it is sufficient to transmit identifications or semi-identifications from each vehicle. The notion of semi-identification has not yet been explained, and will be treated extensively in Chapter 15. For open and closed tolling too, it may be possible to restrict oneself to transmitting identifications or semi-identifications. (As has already been mentioned earlier in the penultimate paragraph of Chapter 5. An example of this is given in Chapter 17.)

9 Security of messages

9.1 Signing messages

The transmission of messages to the authority with relevant data about one's accounts can be seen as a submission of an automated, electronic declaration. If such a declaration turns out to contain errors, intentional or not,

-8 SEP 2003

then one would like to call to account the sender responsible. Thus it is convenient if: 1) the sender responsible can be determined indisputably, and 2) this sender can be called to account as to the precise contents of the declaration. The latter requires that nobody can alter the contents of someone else's declaration unnoticed.

If one wishes to have both properties just mentioned, one must require that every declaration carries an – unforgeable – digital signature. For, a digital signature ensures the authenticity of both the identity of the sender and of the contents of the signed message. In other words, such a signature ensures that one can prove the message was not sent by another person, and also that its contents cannot have been altered surreptitiously by another person. Thus, digital signatures can prevent another person making a false declaration, and also remove any chance of success in repudiating an incorrect declaration submitted by oneself.

The authenticity of both contents and sender, which is ensured by a digital signature, need not of course merely be relevant for electronic declarations, but can also be useful and/or necessary for other, or even all, messages.

9.2 Authorized inspection only

By means of cryptography one can ensure that every message remains secret to anybody but the intended recipient. Thus one can for example ensure that a particular transmitted message, such as, for example, a declaration, is only readable by the addressee. Later we will further address the need for privacy protection against and secrecy towards certain persons or authorities. For now it is sufficient to note that the transmitted messages can be encrypted in order to secure against illegitimate inspection.

10 Identification numbers in messages

10.1 The need for identifications

Often it is the case that a message to be transmitted by vehicle equipment must also include a number of identifications. A number of reasons for this can be given.

In the first place, as will be explained in detail later, it is necessary to be able to verify that the counter value or the counter values only increase and are not occasionally – during traffic participation or while stationary – set back surreptitiously. For this it is necessary to be able to determine whether or not the counter values submitted at various points in time belong to the same FVE, or to the same LVE respectively. Thus, in the approach first described by us, with remote verifications only, a corresponding identification number must be transmitted together with every counter value.

In addition, it must be possible to charge the registered traffic fees to the correct payer regularly. To this end, it is desirable to register or transmit some identification number of the payer with each counter value and/or counter identification. If desired, payments might also be made in an anonymous or semi-anonymous way *within* the vehicle. In view of the need for privacy protection, it may seem attractive to do so, and then just sending a proof of payment together with the counter value or counter values. But even then, the need for identification numbers has not necessarily disappeared. After all, the fee collector, for example, will normally want the proof of payment to specify for which counter has been paid. It does not seem that easy, therefore, to get around the use of some identification number or another when charging.

-8 SEP 2003

Thirdly, it is at least desirable for particular messages, such as declarations, to carry a – digital – signature. However, one can only verify the signature on a message if one can determine to whom the signature is supposed to belong. In short, if a message is signed, the intended recipient must be able to identify the owner of the signature.

In short, some form of identification seems indispensable. How one can ensure a sufficient level of privacy protection despite the use of identification(s) will be discussed in Chapter 13. And in Chapters 15 and 16 we will show that the use of identifications of persons and/or vehicles can be minimized, and how this can be done.

10.2 Several identifications

Several identification numbers may be necessary and various kinds may be used. We will come back to the latter in Chapter 13. If one associates certain counter values with vehicles, then a vehicle identification must accompany such counter values in the messages. In such a case, the counter is actually bound to the FVE and it is thus possible to opt for a FVE identification number instead of a vehicle identification number. Which of the options is more convenient depends, amongst other things, on the desired course of things in the case of, for example, replacement of equipment in the event of defects etc. One can also choose to associate each person with one or more private counters. Then the identification number must concern the person or his counter, i.e. his LVE. When considering this last choice, one should, among other things, bear in mind what should happen in the case of, for example, loss and/or theft of the personal LVE. One might also have two counters be maintained during traffic participation: one associated with the FVE, the other with the LVE. Thus in this case, message transmissions must at least include the two associated identification numbers.

Maintaining a counter per person has a number of advantages. Firstly, several users/payers can take turns in using one and the same vehicle (i.e. can 'share' vehicles), and yet each individual can be charged with the traffic fees due to his/her own use. Secondly, this makes it possible to introduce a quota system, in which each citizen is allowed, for example, to travel a quotum of kilometers in a motorized fashion or to cause a certain quotum of environmental pollution (of some kind). Possibly the trading of all or part of such usage rights or pollution rights will be permitted or regulated.

For convenience, in the remainder of the text we will – almost – always speak of one counter and do so without specifying what kind of counter is concerned. Thus, in the remaining explanation in general we do not distinguish between the various possible cases with one or several counters and with counters that are personal or not. A person skilled in the art is considered to be capable of further supplying the required details in each case.

11 Checks

To make and keep a traffic information system sufficiently fraud-resistant, all sorts of checks [alternative translation: verifications] will, in general, be needed. Of course, one will need verifications in particular on the reliability of data for which, directly or indirectly, some economic interest (say, money) is at stake, such as, for example, in the case of price calculations or traffic fees. An incorrectness or unacceptable deviation revealed by an inspection may, for example, be the result of a fraud attempt, a defect or an incorrect tuning. The counter action may for example consist of stopping the vehicle, or of sending a summons to the holder of the vehicle to bring the vehicle in for further inspection.

-8 SEP 2003

11.1 The fee collector as inspector

Although it is a possibility that the government or the fee collector could contract out certain inspections to various competitive organizations, we will for our convenience often assume in the remainder of this description that the inspector and fee collector are one and the same, i.e. that there is one fee collector who takes care himself of performing the necessary inspections. Therefore, we can restrict ourselves to the term *fee collector* when we wish to specifically refer to the authority. (Often, however, we will just continue to use the more abstract term *authority*).

11.2 Remote verification

An important aspect is that the authority can also verify from some distance, i.e. without obstructing traffic at all, whether the accounts in the vehicle are kept *correctly*. In first instance we will treat one thing and another for the case that the accounting concern only the kilometer counter value. For good verifications on correct kilometer counter values, attention must generally be paid to two aspects, namely: 1) whether the kilometer counter is continually incremented correctly, i.e. whether the kilometer counter is *precise*, and 2) whether the kilometer counter is not being surreptitiously decremented now and then, i.e. whether the kilometer counter is *monotonically* increasing (more precisely formulated: monotonically non-decreasing).

11.3 Checking the precision of kilometer counters

To check on the first mentioned aspect, one can set up an *inspection trap* at randomly chosen, varying (and possibly also at a few permanent) positions. If the inspection trap consists of a section of road where there is no opportunity to leave the road between the beginning and the end of the trap, then it has one entrance and one exit. If after the beginning of the inspection trap there are, for example, a number of forks and/or exit ramps, then the inspection trap can be seen as a tree structure with one entrance as its root and many exits as its leaves. Even more complicated inspection traps with several entrances are conceivable. In any case, the intention is that one can only enter an inspection trap via one of its entrances and only leave it via one of its exits. Besides that, it is important for verifications of kilometer counters that the length of each checking trajectory, i.e. of each trajectory from an entrance to an exit, is known with sufficient accuracy. (An inspection trap can also be used for traffic control, namely for observing and gaining insight into the course of traffic flows. In this case, the lengths of the trajectories inside the inspection traps play no role.)

Of each participating vehicle (or, of each VE) that travels a checking trajectory, the kilometer counter value is read out twice. Once at the moment that the vehicle passes the beginning of the checking trajectory, i.e. enters the inspection trap, and once at the moment that the same vehicle passes the end of that trajectory, i.e. leaves the trap. With the aid of a processor, one can, for each pair of related kilometer counter values, subtract the two numbers from each other and compare the result to the known length of the checking trajectory.

If both distances correspond sufficiently accurately, then apparently the kilometer counter is properly maintained in the vehicle. Obviously, if on the other hand the difference is considered to be too large, a certain action will be initiated. This action may, for example, consist of arresting the vehicle concerned further up the road. Or, for example, of making a video recording of the license plate of the vehicle concerned in order to later track down the holder who is responsible and then summon him or her to bring the vehicle in soon for a further inspection.

-8 SEP 2003

(Note: We anticipatively remark here that manipulating license plates is generally easy to do and that it thus would be advisable to arrange for a really fraud-resistant means of identification.)

Whether two counter values are related, i.e. are associated with either the same vehicle or the same payer, can be determined by providing that each kilometer counter value in a transmitted message is accompanied by a proper identification number or semi-identification number. The term semi-identification number will be treated extensively in Chapter 15.

11.4 Ascertaining the inspection-related vehicle

Before continuing the discussion of kilometer counter verifications, we remark that for certain measures or counter measures, such as, for example, the taking of a photograph, it must be known precisely from which vehicle the unacceptable declaration originates. Furthermore, one must be able to relate an independent measurement (for example, a speed measurement; see also Sections 11.10 and 16.7) to messages from – or, more in general, to communication with – the correct vehicle[32]. In other words, one must then be able to ascertain with sufficient certainty the physical identity – say, the position – of the vehicle with which communication is taking place. A prior art technique, for example, is taking cross-bearings. However, taking sufficiently accurate cross-bearings on one or several messages broadcasted (i.e. transmitted in all directions) by or from the vehicle, may be impracticable or even impossible. Therefore we suggest here the possibility of realizing one thing and another by means of directed [alternative translation: beamed] communication from and/or to the vehicle that is, or is to be, inspected. In particular, 'pointing to' the vehicle in question by means of directed communication towards the vehicle, seems to be a very attractive option.

For the sake of clarity, we give one example in more detail by way of further elucidation. One could aim a narrow beam[33] at one or more receivers, whether special or not, of the vehicle that is to be inspected, in such a manner that only this vehicle receives the message being transmitted via the beam or beams. The message having to be sent in the case of an inspection aimed at a specific vehicle, then concerns an instruction for the checked vehicle, or the equipment in the vehicle, to which instruction of course should be responded immediately and in a prescribed way[34]. Upon reception of the required response (or responses), the verifying authority thus will know exactly which vehicle is 'responsible' for this response (or these responses). If there is no response by or from the vehicle pointed to by the beam (or beams), or if the response is not in time or is otherwise inadequate, then that

---

[32] This is particularly difficult if the messages sent from the vehicle do not contain a fraud-resistant identification that is suitable to relate them unambiguously to the correct independent measurement.

[33] For example, a beam of electromagnetic waves. The only requirement is that the communication can be aimed, i.e. that the beam can be made sufficiently narrow. Another possibility is to use several beams and to ensure that at the moment of inspection only one vehicle is covered by all the beams. We do not pursue this matter further, as this remark should suffice for a person skilled in the art.

[34] In the instruction one might include, for example, a unique number, say an instruction number, and one could make it obligatory to mention this number in the response or responses to this message. Also one might require that the response or responses have to be signed. The latter is advantageous for later furnishing of proof, but is disadvantageous for the anonymity of the sender.

will of course constitute an offense that induces a counter measure (such as, for example, stopping the vehicle and/or sending a summons for an extensive inspection).

At the risk of being superfluous, we remark that this technique is not only applicable and of importance in case of TIP systems, but also more in general. Particularly also in case of positioning-based systems using a GPS and/or an electronic roadmap. If it turns out that the verification technique (or the application of the verification technique) as suggested by us, using directed communication and active participation of vehicle equipment, is indeed new, or is new in the context of the said traffic information systems (that enable continuous pricing), then we wish to claim this technique (method) as extensively as possible. Thus, it is, among other things, explicitly our intention that the use of this technique for positioning-based traffic information systems using GPS and/or an electronic road map also forms part of our invention.

11.5 Checks against surreptitious reversal

To ensure that counter values do only increase monotonically, i.e. that they cannot be set back at any moment without real danger of being caught[35], there must be a sufficient number of checks on counter monotony. These verifications take place by reading out counter values with accompanying identification, i.e. intercepting declarations, at random times, thus also at the most unexpected moments. Upon reception of a declaration, accounts to be kept by the inspector will be used to find the counter value that until now was recorded as most recently received relating to the identification in question. If the currently received counter value is higher than the one found in the accounts, it will be registered in the accounts as the most recent one. If it is lower, an appropriate counter measure should be taken, as this signifies an unpermitted situation.

The accounts needed for monotony inspections thus consist of one most recently intercepted counter value per identification. It should be clear that each counter value must be uniquely identified again and again by one and the same identification, and that the use of real identification numbers is essential to these monotony checks. Semi-identification numbers therefore are not suited for this. This last aspect should become clear to the reader after reading of Chapter 15.

Please observe that for monotony checks it is sufficient to intercept messages transmitted from vehicles. Thus, for these checks it is not necessary to determine the position of the vehicle at the moment of reception of the message, as is necessary in the case of checks on precision.

If the counter value or values are identified in each message by identification numbers, then it will be possible to combine, in each inspection trap, precision checks with monotony checks. It is thus not always necessary to perform 'separate' checks on counter monotony.

11.6 Checking counters in general

The method described above for checking on monotony can be used not only for kilometer counters, but for other kinds of counters as well. Furthermore, it cannot only be applied in the case of increasing (incremental) counters, but obviously also in case of decreasing (decremental) counters[36]. In short, the monotony may equally well be

---

[35] In particular, protection against setting a counter back during a standstill is also necessary!

[36] Decremental counters may, for example, keep track of the kilometers or 'pollution rights' still available.

decreasing instead of increasing. For complete verification, checks on precision are required additionally. But fortunately, checks on precision are also possible for far more counters than kilometer counters only.

Suppose for example that there is a question of a traffic fee counter and that the amount of 'levy points' for a traveled distance unit is a function of several variables, such as, for example, speed, engine speed, vehicle type, length, width, and the like. As long as the correct value of all used variables can be determined reliably, the traffic fee counter can be completely verified. The values of variables involved can be ascertained reliably in two ways, namely either 1) by determining them externally, i.e. independent of the report from the vehicle (and remotely), or 2) by making sure that the report from the vehicle can really be trusted. In the following three sections we digress somewhat further on this.

In passing, we remark here further that, for data that can be determined externally, their presence in each declaration does not have to be required, strictly taken. However, it is usually more convenient to do so anyway. After all, checking whether a reported value is correct may be easier – and therefore cheaper – than independent ascertainment, but never more difficult (or more expensive). For example, checking whether a reported registration number is in accordance with that on the license plate is easier than reading the registration number on the license plate totally independently (i.e. without having any hint).

Finally we note that, in case of separate checks on precision and monotony, it must be prevented that a certain counter in a vehicle can escape from a full check by giving the appearance of two different counters. In other words, one must make sure that both kinds of checks for each individual counter can be correctly 'associated with each other.'

11.7 Data suitable for remote verification

The detection of incorrectnesses or deviations is at least possible for all kinds of data, supplied by vehicle equipment, of which the correct values can be remotely (and preferably automatically) determined for passing vehicles. This can be done by *direct* determination, such as, for example, with speed, speed change, length, width, color, shape of body-work, registration number on license plate, and the like. Sometimes it can be done *indirectly* via derivation from other data.

An example of this, already given before, is the fuel consumption. Even though the fuel consumption of a passing vehicle cannot be directly measured remotely, it is often possible to derive the fuel consumption rather accurately from a number of other data that have proven to be highly determining for the fuel consumption of the passing vehicle. For these other data, think, for example, of the full classification of the vehicle and of certain data about the use – including the usage conditions – of the vehicle, i.e. certain data related to its movement. As already mentioned, a full classification can, for example, consist of brand, model, year of make, gearbox and engine type. Usage data that may play a role, are, on the one hand, for example, speed, acceleration, engine speed, and the like, and on the other hand, for example, the air humidity, air pressure, outside temperature, wind speed and wind direction. If a sufficiently accurate relationship is known, and if reliable values are also available for the thereto-required data (i.e. for the input parameters), the correct fuel consumption thus can still be derived. A value reported from a vehicle can thus really be verified for reliability.

Another example of a derivable datum is, for example, the engine speed. If a full classification (make, model, year, gearbox and engine type, and the like) of the passing vehicle is known, one can check indirectly in what gear is being driven by performing a speed measurement, a speed change measurement (say, an acceleration

- 8 SEP 2003

measurement) and a directed sound measurement. Based on the speed and the data made available by the manufacturer (and perhaps checked by the authority) concerning transmission ratios, one then can derive the engine speed much more precisely and use this for verifying the correctness of the reported engine speed.

We have already stated that various counters can be spot-checked remotely and described how this can be done. It should now be clear that revolution counters and fuel counters also belong, or can belong, to that category.

11.8 Another example of the usefulness of derived information

To illustrate the possibilities that derivations can offer, we describe here in passing yet one more specific example. This example concerns the possibility of deriving the total amount of noise caused by a vehicle (thus including noise resulting from airflow around the vehicle) rather accurately from a number of other data. The nice thing about this example is that derivation may even be necessary, because in certain cases it seems unfeasible or even impossible to actually measure this datum sufficiently accurately.

After all, in the case of road traffic one may be hampered a lot, both in the case of measurement from the vehicle itself and in the case of measurement at a certain distance along or above the road, by the noise produced by possibly heavy ambient traffic. Besides, it seems impossible to measure the noise of the self-produced air turbulence from a fast moving vehicle. The latter in particular also plays a role in case of air traffic. By the way, in case of air traffic sufficiently accurate noise measurement seems only unfeasible from the concerning airplanes themselves.

Note that the difference with respect to the example, mentioned before, of environmental pollution caused is that, at least in case of road traffic, it is in principle really possible to actually measure and analyze the exhaust fumes in the vehicle. In that example we assumed only that actual measurement and analysis was too expensive.

11.9 Data not suitable for remote checking

Of course one might also have the vehicle equipment use and transmit data of which one does not know (yet) how these can be directly or indirectly remotely verified in a sufficiently easy and therefore sufficiently cheap way for vehicles participating in traffic. For such data, think, for example, of the type of engine that is present in the vehicle, the position of the gas pedal and/or whether the engine uses LPG (Liquefied Petrol Gas) or gasoline. (Nevertheless, it is indeed imaginable that the position of the gas pedal can be indirectly verified if sufficient other factors are known. Also, the exhaust of a vehicle might be 'sniffed at' sufficiently well at some distance to establish a distinction between the use of LPG and gasoline without disturbing traffic.)

If the correctness of such data is of sufficiently high importance, it must be made sure that these data are obtained, collected and transmitted in a sufficiently fraud-resistant way. For example, in order to prevent false input to the processor (of the VE), the components involved in collecting that kind of information – often sensors and their connections to the processor – must be so engineered to be sufficiently fraud-resistant[37].

---

[37] Since the whole chain up to and including transmission must then be protected against fraud, the processor will almost certainly have to be fraud-resistant as well. Anyway, we here are actually just anticipating on the later treatment of the use of agents.

-8 SEP 2003

In short, for every kind of data used that can not or not sufficiently easily be spot-checked – and with our first approach: remotely – with moving traffic, a sufficient guarantee of the reliability by means of physical protection seems required![38] If, for example, a reliable report from the vehicle about the registration number and/or the full classification of the vehicle is considered to be necessary for the desired traffic fee system, these data can be held and supplied in a sufficiently fraud-resistant way by a component, installed, for example, under seal. It may concern a separate, special component for just this purpose (i.e. what we will call a specialized agent in Chapter 16), but a – general – agent that is attached to the vehicle in a fraud-resistant way, can also perform this task. We will return to one thing and another in Chapters 14 and 16.

11.10 Checks based on difference quotients or derivatives

We have illustrated with the above that it is, more in general, possible to carry out checks on precision by taking delivery of a value at each of two points to be passed successively, and by seeing whether the difference between the two reported values agrees with a reference or calibration value that has been obtained in a different, reliable way. The reader has probably sensed the suggestion (and not unjustly) that these two points must be at a certain distance from each other. However, the moment now seems to have come to point out explicitly the possibility of carrying out checks with the help of difference quotients or derivatives [alternative translation: differential quotients]. Put differently, in principle one could choose the distance between the measuring points to be very small, and one could let difference quotients or derivatives be transmitted from the vehicle. In Chapter 16, we will illustrate this possibility by showing that verification of a kilometer counter can also take place by using the correct speed at a certain moment (instead of the correct length of a checking trajectory) as a reference value or calibration value.

11.11 Roller test bench for further inspection

If, based on a check, something appears to be incorrect, the vehicle in question and particularly the vehicle equipment in question must be further inspected and verified. Also, one may embed in the law the obligation to have every vehicle undergo such a further inspection periodically, for example at least once a year. In addition to a visual inspection for defraud (or attempts thereto), the further inspection may consist of testing for the correct functioning of the vehicle equipment on a roller test bench developed for that purpose. With the roller test bench, all kinds of situations can be simulated and the correct functioning of the vehicle equipment in those situations can be checked or the cause of incorrect functioning can be traced.

12 Use of a receiver

If every participating vehicle is also equipped with a receiver, then this gives a large number of possibilities and advantages, of which we mention only a small number here.

---

[38] As we have already shown earlier, we are of the opinion that it is in general wise to rely as little as possible on physical protection (alone), because, among other reasons, a high level of physical security often goes hand in hand with high costs.

-8 SEP 2003

12.1 Automatic calibration

For example, transmitters along or over the road can transmit information (for example on the speed of the vehicle, or on the correct distance between two points to be passed) that makes it possible, after reception in the vehicle, to calibrate certain equipment (in our example the kilometer counter and the speedometer) automatically.

Thus, one advantage is that kilometer counters and speedometers can be calibrated fully automatically while driving on certain road sections, so that they continue to work accurately all the time. In this way, the influence of tire wear on the accuracy of kilometer counters and speedometers might even be removed. In a similar way, for example, a thermometer that is attached to the vehicle to determine the outside temperature can also be made self-calibrating, i.e. check itself automatically and/or adjust itself based on a transmitted reliable temperature for the location of the vehicle. By ensuring that the thermometer in a vehicle can register the outside temperature more accurately, there could, for example, be a more accurate warning for possible slipperiness as a result of freezing.

It is self-evident that other measuring equipment in vehicles can also be calibrated automatically in a similar way. The reverse is also possible, namely that measurement equipment along the road calibrates itself, i.e. checks itself for correct functioning and/or adjusts itself automatically, based on the measurement values provided by passing vehicles. After all, one might calculate a value, such as, for example, the temperature, at a certain location fairly accurately based on a sufficient number of values measured and supplied by passing vehicles. So, the automatic calibration of the measurement equipment, such as, for example, speedometers and thermometers, can concern measurement instruments in vehicles as well as measurement equipment along the road, and it might even be done mutually.

12.2 Some other advantages

The use of a receiver also makes it possible to prevent the clock from deviating too much in the long run, and to handle time changes (when crossing a time zone border and when changing from summer daylight saving time to winter daylight saving time or vice versa) automatically. Because speed is a quantity derived from the distance traveled and the time, the measurement of the speed in a vehicle can be done with extra accuracy if it is known by how much its clock speed deviates.

Further it is possible to use a different calculation method for every tariff area, consisting of a certain road section or of all the roads in a certain area. Thereto, one may have transmitters at *all* the crossings of borders between tariff areas to inform passing vehicles of the tariff changeover. Another advantage is that a new calculation method, i.e. tariff function, can also be received. This can be used, for example, to implement a tariff increase or to adjust the valid peak times.[39]

The transmitters of the infrastructure (often along or above the road) and the receivers in the vehicles could also be used for the distribution of new software in general and of new software on behalf of the traffic information system in particular. By ensuring that software provided with a correct signature can be installed and put into

---

[39] A receiver can be used beneficially with the examples mentioned here, but it is not absolutely necessary. For example, a tariff change when entering a different tariff zone can also be set manually or be done automatically with the aid of a GPS.

-8 SEP 2003

operation automatically to replace an earlier version, certain changes or adjustments might be made even without intervention of the user or holder of the vehicle.

The receiver can also be used to limit the transmission from the vehicle to a short period after every authorized request. Probably the most important advantage of this is that less bandwidth is necessary for the communication with all vehicles. For the protection of privacy, this has the advantage that it becomes somewhat more difficult for third parties to eavesdrop on the message traffic. Furthermore, possible attempted misuse by the government (for example, an attempt to still trace all traffic by putting a transmitter/receiver on every street corner) will become more conspicuous or will be easier to detect. On the other hand, is it a disadvantage from the viewpoint of fraud prevention if one can find out in every vehicle at what moments and/or locations data are requested by inspectors. After all, without extra counter measures, the protection against fraud by spot-checking will then generally become weaker, because one can then anticipate or gamble better on moments at which tampering with the counter will probably not be discovered. (See Chapter 16 for further details.)

It thus seems that, in the case of only remote checking, one must make a choice between either 1) a simpler fraud prevention and more use, or more need of the use, of cryptography to protect against eavesdropping, or 2) more difficult fraud prevention but less or maybe even no use, or need of the use, of cryptography for the privacy protection. Because cryptography will often be required anyway, for example in order to maintain the secrecy of messages and/or to provide digital signatures on messages, the scales may tip in favor of (almost) continuous transmission when making this choice. However, the approach described in Chapter 16 without continuous transmission from vehicles, but with supervision by agents in vehicles, offers a very attractive alternative. By the way, this latter approach usually does indeed make use of receivers in vehicles.

Of course the receiver can be used for many other purposes as well. For example, on reception of a certain code or of an appropriate message signed or co-signed by the holder or owner, a switch could be made to adding a full identification to each message transmitted and possibly also to the continuous transmission of an identification. Such a provision can be used, amongst other things, for tracing vehicles after, for example, theft. It is, for example, also possible to inform passing vehicles frequently via transmitters along the road on, for example, tailbacks and delays, or on the locally valid speed limit. The given speed limit can, for example, be used to warn the driver when he is speeding. The following section describes how traffic safety can be increased by having speed limits respected automatically.

12.3 Automatic respecting of official speed limits

We propose to implement the equipment for cruise control in such a way that it is able to start using the messages disseminated by the traffic information system regarding speed limits. In this way the driver can be relieved of a part of his task, because the maximum speed to be driven can then be adjusted and obeyed automatically. Adjustment to a higher maximum speed will then normally only happen if this maximum allowed speed is still lower than the desired speed that the driver has set for cruise control.

Such a provision will no doubt benefit the traffic safety. The task alleviation for the driver alone could already ensure a positive effect. In addition, accidentally exceeding the official speed limit, for example because the driver misses a traffic sign with a speed limitation, is prevented. Besides, the speed of vehicles can likewise be gradually adjusted when approaching a tailback, and in a tailback the speed of the vehicles can be made fairly homogeneous and even.

-8 SEP 2003

When, in the long run, all vehicles are equipped, or can be equipped, with such equipment (at an acceptable cost), a better basis for strict enforcement of maximum speeds will arise as well, because there will then no longer be a reasonable excuse for speeding accidentally. By strict enforcement, which will become very well possible with the traffic information systems proposed by us, traffic safety can increase even further. Think, for example, of enforcing the speed limitations in residential quarters or residential areas.

Finally, a substantial cost saving will be achieved as well when less speed ramps (first in construction and then in maintenance) and other speed-discouraging provisions prove to be necessary. Besides, think also of the savings as a result of reduced wear of, for example, springs and shock absorbers and of the saving in fuel consumption. (The current practice of braking before and accelerating again after a speed ramp is also extra damaging to the environment.)

Note that such equipment for cruise control also offers drivers the possibility to drive, if desired, as fast as possible without exceeding a speed limit anywhere. Although at first sight this may seem to be an application that is unfriendly for traffic safety, it can definitely still benefit traffic safety! After all, in practice it happens all too often that one wants to go somewhere as fast as possible. If drivers without such an aid try to drive manually as much as possible at the maximum allowed speeds, that will cost a high level of attention and concentration, while they will still unwillingly exceed the maximum speed every now and then. With a mass use of this facility on highways, the speed variations and differences will decrease, which will benefit traffic safety additionally.

12.4 Entry support for highways

The collaboration between the TIP system and the cruise control might go even further in the long term. For example, support could be offered for entering a highway. The traffic information system can then, for example, determine an entry position between the vehicles already driving on that highway and, if necessary, influence the speed of those vehicles and of the entering vehicle in such a way that merging takes place safely, smoothly and without problems. We will not go further into the details of this.

13 Privacy protection

In this chapter, we will pursue the matter of how payments and verifications can be arranged and how at the same time sufficient privacy protection can be offered. We base our explanation primarily on the situation in which the traffic fees are settled via giro or bank account, for example by means of automatic payments based on a prior authorization. Later we will also glance at the possibility of direct payment in the vehicle by means of a chipcard.

As mentioned above, we assume that the fee collector also functions as inspector. In the event that verifications would be contracted out to several independent organizations, the privacy of the traffic participants is less threatened, so that it then will be easier to protect privacy. Thus, we limit our explanation here to the more difficult case in which the fee collector himself is the only inspector.

13.1 Direct and indirect identifications

For the identification of a payer there are several possibilities. For payment it is not necessary that the authority, in this case the fee collector, knows exactly who is the payer. So, a *direct* personal identification, as is the case when using a driver's license number, passport number or social security number, for example, is not strictly necessary and even can be undesirable. From the point of view of privacy protection, it is generally better to use a

8 SEP 2003

suitable *indirect* identification (think, in this regard, of a bank account or credit card number, for example), so that the fee collector does know where the bill should go to, but not also immediately knows who is covered by this identification.

Normally, the organization that has issued a certain indirect identification number for this purpose, will keep secret, or have to keep secret, which person is covered by that number. Of course, this requires legislation that also describes in which circumstances the organization concerned may, or must, reveal the identity of the corresponding person.

Note that it is not true that any indirect identification will do. For example, if each vehicle has one corresponding holder (owner), the vehicle's registration number identifies the holder of a vehicle indirectly. Nevertheless, registration numbers do not guarantee sufficient privacy protection to holders if the license plate number registration is, as usual, completely accessible to the government. (Of course one could also consider removing the association between vehicles and holders from the license plate number registration of the government, and to protect privacy by delegating this association to one or more separate organizations.)

13.2 Fraud-resistant components, e.g. chipcards

The addition of some identification number may, at first glance, seem unacceptable for the desired privacy protection. However, there are various possibilities to protect privacy sufficiently while still using identification numbers. One interesting possibility concerns the use of chipcards, or other combinations of hardware and/or software, whose fraud resistance the authority is willing to trust[40]. Henceforth, we will only speak of chipcards, although the explanation is also valid for all kinds of other manifestations, including, for example, chipkeys.

In case of securing chipcards against all sorts of fraud, some kind of physical protection will always be present. For example, if, as usual, cryptography is used for the protection of the chipcard and of its functioning, then the card will contain at least one key (i.e. one bit pattern) of which the secrecy can only be warranted by physical protection. Therefore, if a system uses chipcards, the security of the overall system depends also on – the quality of – this physical protection. In practice, this does not appear to pose any difficulties, as in case of chipcards one apparently can provide for a sufficient physical protection against theft of a – cryptographic – key.

Anyway, the organization that issues the chipcard, can incorporate enough safeguards to undauntedly guarantee that the chipcard only functions, and can be used, as intended. As a consequence, it is, for example, possible to let anonymous payments be performed by means of such a chipcard. We assume that the use of such chipcards for anonymous or semi-anonymous payments is already sufficiently known and that it is not necessary to describe in more detail how such anonymous or semi-anonymous payments can contribute to a sound and secure TIP system in which privacy is sufficiently protected. Nonetheless, we will now digress somewhat further on a number of relevant aspects of the possibility of using chipcards for other purposes than payments. The further treatment of the possibility of using chips in general, and chipcards in particular, for example for trustworthily or more trustworthily providing data from a vehicle, will take place in Chapter 16.

---

[40] In this section and the two next ones, we anticipate slightly on the later treatment of the use of agents.

-8 SEP 2003

13.3 Anonymous, anonymously delivered or semi-anonymously delivered chipcards

Chipcards can be anonymous or be delivered anonymously or semi-anonymously. We refer to a chipcard as being anonymous if it is not – sufficiently uniquely – identifiable. The holders of such a chipcard and/or vehicles in which such a chipcard is used, can self-evidently not be identified exclusively on the basis of the card used if this card is anonymous. But also if every chipcard itself really is identified by means of a unique identification number, i.e. if it is not anonymous, identification of the holder of the card and/or of the corresponding vehicle can be avoided. This can be arranged by delivering such identifiable chipcards anonymously or semi-anonymously. We speak of *anonymous delivery (issuance)* if the person or vehicle for whom or which, respectively, a certain chipcard has been issued, whether or not upon payment, is not registered. In the case of *semi-anonymous delivery* this is indeed registered, although by separate organization(s) that act as privacy protector(s). In this case, the association between chipcard and holder and/or vehicle may only be disclosed under conditions that are clearly described by law, and even then only to the government. (This is, to a certain extent, comparable to the issuance of, for example, secret bank account numbers or secret telephone numbers.) In the case of semi-anonymous delivery, we can therefore speak of a form of indirect identification.

13.4 Privacy protection when using chipcards or chipkeys

It would carry us too far to treat exhaustively all possible ways in which with the aid of anonymously or semi-anonymously delivered and/or anonymous chipcards a sound and secure TIP system can be obtained in which privacy is sufficiently protected. We now only point out the possibility of making fraud, or certain forms of fraud, impossible by invoking the help of a chipcard for the – verified – supply of data from a vehicle, such as, for example, kilometer counter values. In fact we here are already discussing an approach using agents, to which we will devote an entire chapter later on. Since chipcards can act as agents, as will become clear later on, we also actually provide in Chapter 16 a further illustration of this possibility of using chipcards. This later illustration is considered to be sufficient for persons skilled in the art.

At this moment, it is actually only of interest that the reader already appreciates that it is easier to protect privacy with the use of anonymous, anonymously delivered or semi-anonymously delivered chipcards than without. In the following, we now provide an extensive explanation of the more difficult case in which no use is made of anonymously or semi-anonymously delivered chipcards or anonymous chipcards to represent persons and/or vehicles.

13.5 Privacy protection when using personal or vehicle identification numbers

As remarked before, the addition of an identification number may seem at first sight to be unacceptable for the desired privacy protection. Above, we have already suggested that privacy can rather easily be protected if the identification number identifies an anonymously or semi-anonymously delivered chipcard. In the following, we will show that one can also offer sufficient privacy protection if the identification number does indeed identify a person or vehicle.

The point is that it is well possible to prevent one from being able to trace systematically the movements of the vehicle and/or the payer. We will show that this can be done in particular by creating a chain of organizations, in which case we will draw a distinction between hunters, intermediaries (specialized privacy protectors) and the eventual addressee/addressees or message recipient/recipients, whom we will occasionally call *final recipient* or

- 8 SEP 2003

final recipients respectively. (As mentioned before, we do not make a distinction between inspectors and fee collector, so that in our example of traffic tax the fee collector is the final recipient.) Messages are in this case only being delivered to the final recipient after intermediation of a hunter and one or more intermediaries. Of course, all kinds of other solutions/variations are also possible. For example, one or more of the ideas that are hidden behind what is explicitly sketched here, may be combined in another way to arrive at a sound and secure system.

13.6 Hunters

The idea is that the authority or the fee collector may not find out at which locations the senders of the messages were at the time of the reception of the messages concerned. We will assume, and in practice this usually will also be the case, that during reception of a message one can determine the location of the sender fairly well. Therefore, at first sight it seems essential that the authority – or the fee collector or, more in general, the government – should not be given direct access to the messages transmitted by the traffic.

For completeness we remark beforehand that this does not necessarily mean that the authority in question, for example the fee collector, will not be allowed to collect the messages on his own. After all, this can do little harm if intermediaries (see later) are used and the contents of each message are unreadable for that authority (or that fee collector) at the moment of collecting. Although we are primarily concerned here with the secrecy of the location of transmittal of a message, the secrecy of the contents of a message thus really is an important aspect as well. One thing and another will soon become clear or clearer.

Anyway, for the sake of taking delivery of messages from as many participating vehicles as possible without interfering with the traffic, one may call into existence independent, mutually competing organizations that offer themselves to the government as 'hunters'. In the case that the final recipient is, for example, a verifying authority or fee collector, he probably will pay the hunters for, among other things, picking up messages from as many participating vehicles as possible and/or for doing so at the most exceptional locations.

For this purpose, each of these hunters may install at various fixed locations receivers for continuous use. Besides, each hunter may also install receivers temporarily at varying locations and times. These last-mentioned receivers thus are moved regularly. Finally, a hunter may also use receivers that are moving continually (for example, because they are driven about), to ensure that vehicle equipment functioning incorrectly (due to fraud attempts or otherwise) has as much chance as possible of being 'caught'.

The fanaticism with which messages are being hunted for, is emphatically of importance for achieving good verification. In first instance, it seems wise not to let this task be performed by the verifying authority itself, but to move this task from the public to the commercial domain and to ensure that the hunters are kept 'sharp' by introducing competition. By making the height of the hunting remuneration dependent on the success of the hunter, 'sharpness' may be additionally stimulated.

Through regulations, one can arrange that each individual hunter must restrict himself to a 'light armament', i.e. that he must confine himself to a sufficiently small network of receivers with a certain geographic spread. Nevertheless, the total network of all hunters may be very extensive indeed, of course. The set-up with independent hunters thereby has a number of advantages with regard to the protection of citizens against their own government: 1) the government has no direct access to any receiver in this network and therefore requires permission by a hunter to be able to utilize a particular receiver in a legal way, and 2) the government can only obtain access to

- 8 SEP 2003

a substantial part of this network in a normal way in cooperation with several hunters, so that even conspiring with one or a few hunters does not pay off or hardly pays off.

All in all, the described set-up affords a certain protection against possible attempts by the government yet to be able to trace the traffic rather well, if need be in an illegal way, by means of a very dense network of receivers. For, the government cannot use the network of the hunters without further ado and thus either has to 'break into' a very large number of receivers of that network, or has to create, especially for this purpose, a network of receivers of its own. Both possibilities seem to be rather costly and also seem to be almost impossible to be implemented unnoticed.

Finally, we remark that one, to be quite on the safe side, can oblige hunters to keep secret the location of reception (or, better formulated, any possible indication of the location of the sender at the moment of reception) of every message intercepted by them. Additionally one might possibly also prescribe that for certain kinds of messages the precise time of reception must be kept secret as well. Of course, one can – and in general will – make a number of precisely described exceptions to these obligations.

An extreme case is that hunters will be legally forbidden to even register the location – and possibly the precise time of reception – of messages[41]. However, it is also possible, for example, to dictate that hunters may and must register, only during a certain limited period after reception of each message, where the sender must have been at the moment in question, while, at the same time, deviation from absolute secrecy is allowed only, for specific cases and in a prescribed way, in circumstances clearly described by law. We will return later to the use of such a registration for the benefit of interventions at the proper location, such as, for example, video shots.

13.7 Intermediaries as privacy protectors

Although in the above-mentioned way a reasonable protection can already be offered, we need not be satisfied yet. After all, the primary interest of the hunters does not always have to be the privacy protection of citizens, certainly not if they are paid by the fee collector or, more in general, the government. Moreover, we want a better protection against the possibility of the government being able, through a network of receivers of its own, to obtain more information than some people care for.

We will now show that an important contribution to the total protection can be made by having all messages coming from the traffic enciphered in such a way, that neither the government, nor others can read their contents without first getting help from one or more independent, privacy-protecting organizations, which we will henceforward call intermediaries. The purpose of the use of intermediaries is to hinder the undesired tracing of vehicles and/or responsible payers as much as possible.

The idea is that the holder of each vehicle and/or each payer himself, from now on both to be called *sender*, chooses at least one intermediary, who will then furnish the desired service. (We will here not go further into the matter of how the intermediary gets paid for furnishing these services.) The mandatory messages, to be sent from a vehicle, will then, before transmission, be enciphered by the sender in such a way, using cryptographic tech-

---

[41] Later it will become apparent that it would be more appropriate not to let hunters also act – or partly act – as intermediary. In the case of these 'pure' hunters, such a legal prohibition would not seem far-fetched at all. See further on in this chapter.

-8 SEP 2003

niques, that they can only be deciphered by the chosen intermediaries. Almost the only thing that intermediaries have to do is to decipher the messages destined for them and delivered to them via hunters, and to subsequently forward these deciphered messages to the final recipient (for example, the fee collector) or the next addressee on the route to the final recipient.

An essential point is that by means of cryptographic techniques it can be ensured that only the intermediary chosen by the sender will be capable of deciphering the message in question. Furthermore, for outsiders, even if they can eavesdrop/intercept the message stream to and from a certain intermediary, it is impossible to figure out which incoming message belongs to which outgoing message of that intermediary.

In the following we will limit ourselves in our further explanation to the case that the whole message is made anonymous. Of course it is also possible to apply the described techniques only to a part of the original message.

More in detail, the service that intermediaries must provide, in general consists of: 1) deciphering each message that they receive via a hunter and possibly other intermediaries, i.e. removing the protection against reading (by anyone else but the intermediary) from the message in question, 2) forwarding the deciphered message to the next addressee (for example, the final recipient), and 3) keeping secret the relation between incoming and outgoing messages. In later sections we will explain that intermediaries, if necessary, will also 4) keep certain accounts about the relationship between incoming and outgoing messages in order to be able to send back a possible reaction of the final recipient, to the message received by him, via the reversed route to the hunter through which the message had come in. Later we will see that, if the message comes from a 'pure' hunter, the – first – intermediary in addition has to remove first of all the location and the point of time.

The third point mentioned states that these accounts must be kept secret. The specific cases and circumstances in which one may deviate in a prescribed way from absolute secrecy, may be clearly embedded in law. It can also be embedded in law that intermediaries for each message may or must register this relationship only for a certain limited period of time after reception.

By calling intermediaries into existence as sketched above, one can arrange in a reasonably simple way that the privacy (at least as far as movement patterns are concerned) will not be violated, not even if we assume that the hunters can locate the sender of a message. The latter will, in general, be the case if the receivers are placed alongside or above the road.

13.8 Intermediary varying per message

We point out that one does not have to choose for one fixed intermediary and then be dependent on the integrity of this single organization for one's privacy. After all, one can also choose several, and possibly even all, intermediaries from the ones available, and then make a random choice from the pre-selection made for every message to be sent. The messages then run via continually varying intermediaries. In other words, the stream of messages of such a randomly choosing client is 'cut in pieces' and spread over various intermediaries, which will certainly benefit the privacy protection. After all, even if a certain intermediary conspires with a hunter to illegally find out one thing and another about the movement patterns of such a client, then these two still can capture only a small, random part of his message stream.

-8 SEP 2003

13.9 Messages only readable for the final recipient

By the way, one can ensure that no intermediary and/or hunter can read the contents of the messages and therefore that they cannot or can hardly get information on movement patterns. After all, the messages additionally can be obfuscated in such a way that, after being deciphered by the intermediary, they can be read only by the next addressee (for example, the final recipient). Thus, the hunters and intermediaries then simply take delivery of messages and process those messages without further being able to understand anything of the contents of the messages.

In this case, messages (or parts of them, although we have already excluded the explicit treatment of such a case) are thus – at least – doubly enciphered. Once to make the message only readable by the actual, say second, addressee, and once more thereafter to pack the message in such a way that this second addressee can only read it with the help of, that is, after deciphering by, the intermediary, i.e. the first addressee. In short, as long as an intermediary does not conspire with the second addressee (say, the final recipient), this intermediary cannot distil any information from the contents of the received and forwarded messages.

In the way just described, where the whole message is always obfuscated for anyone but the final recipient (or the next addressee), there is no danger at all to be feared from the intermediaries and/or the hunters.

13.10 Several intermediaries for one message

Of course the privacy of a randomly choosing client now still can be violated for a small part if an intermediary conspires with both a hunter and the final recipient, at least if the latter is the second addressee. But by using a series of addressees and applying the corresponding series of encipherments to a message, one can ensure additionally that a message will pass via a number of successive intermediaries. For example, in case of three intermediaries between the hunter and the final recipient, the privacy can only be violated if all five mentioned organizations conspire. If one always chooses the intermediaries to be used anew and randomly for each message, then such a possible violation still will concern only a small, random part of the stream of messages sent by a certain sender.

Note, by the way, that the use of one intermediary for a message already seems to offer sufficient protection and that in practice there will probably be little need to use more than one intermediary for a message, at least for some time to come.

13.11 Return messages, such as requests for a counteraction

In some cases it is necessary, for example, to take a video shot, or to have a video shot taken, of the vehicle associated with a transmitted message. If something is wrong with the transmitted message, say a declaration, but it has been signed correctly, then the final recipient, say the fee collector, can identify the one responsible and thus usually also track him/her down. Thus, a counteraction in the form of, for example, an arrest or a video shot then does not seem to be necessary. But if it concerns a declaration or a message without a correct signature, then a counteraction, such as, for example, an arrest or taking a video shot, should be initiated at the place where the vehicle is located.

This is possible without the final recipient getting to know the location of the vehicle. We will outline explicitly one relatively simple possibility that goes as follows. According to legal regulations, every hunter assigns a unique number to a message upon its reception, and then registers this number for a short period of time together

with – an indication of – the location of reception (or with – an indication of – the location from where the message has been sent). The message itself need not or may not be retained by the hunter, but does have to be forwarded to the specified intermediary with said number attached to it.

Each intermediary removes this number from each incoming message, takes care of 'unwrapping' the message and then forwards it to the next addressee with another unique number attached to it. Each intermediary retains for a certain time the combinations of incoming and outgoing message numbers that are related to each other, and from whom the incoming message was received.

If the final recipient wants to have a video shot taken of the vehicle in question, for example, then he sends to the intermediary from whom he received the rejected message a signed request for such a counteraction, mentioning the message number earlier attached to the message by this intermediary. (That the request must be signed has to do with preventing abuse of this possibility.) In his accounts, the intermediary looks up which incoming number corresponds to this outgoing number once chosen by himself. Next, he forwards the request, together with the found incoming number, to the corresponding, registered sender.

In this way, the right hunter will eventually get the request. In his accounts, the hunter looks up the right, corresponding location and initiates the counteraction, say the video shot, at that location. Thus, hunters are not only paid for hunting messages transmitted from vehicles, but also for carrying out counteractions upon authorized request, i.e. for the 'hunt' (or a part of the 'hunt') for possible violators.

13.12 'Opening' locations for the benefit of inspections

For carrying out certain inspections, in particular for checks on the correct functioning of kilometer counters, it can be desirable that the inspector knows what the distance is between two locations that a vehicle passes successively. For this purpose one may temporarily withdraw the secrecy of a number of locations. Thus, the inspector will even in this case surely not get unrestricted access to the information on the locations of reception, but must each time apply in advance for such access for a number of checkpoints. Obviously, access will then only be granted for a limited time and with regard to a limited number of varying locations.

13.13 Hunter preferably not as 'semi' intermediary

In case of the arrangement of the whole chain as described above, the hunters take care already of the privacy protection, or a part of the privacy protection, by partly also operating as an intermediary. The only substantial difference between a hunter and a 'normal' intermediary is actually that the client does not choose the hunter himself. Thus, if there are several hunters, it is also impossible to send secret messages to the hunters, because the client does not know beforehand which hunter will intercept the message.

With a somewhat different and actually also purer and better approach, a hunter does not act at the same time as a 'semi' intermediary. In this approach the hunter adds to each received message the location, date and time of reception and signs the thus resulting message. It is then no longer necessary for every hunter to keep accounts to be able to specify later at which location the delivery of the message had been taken, or at which place the vehicle was located during the transmission of the message. (Even stronger, this can then even be forbidden.) The first intermediary in the chain retains the complete message signed by the hunter, but only forwards the original message, transmitted from the vehicle, to the next one in the chain. Thus, the retained message registers the location of the vehicle at the time of transmission, or the location of reception by the hunter, and can, if necessary,

-8 SEP 2003

later be brought up as a piece of evidence. The latter is an advantage with respect to the variation previously sketched.

Note that a final recipient – such as, for example, a government agency – now might operate himself as 'message hunter' without the privacy protection necessarily being jeopardized. For a really good privacy protection, it does remain necessary to deny the government unrestricted access to certain things, such as, for example, video cameras along the road. Certain counteractions – such as, for example, taking video shots – should therefore preferably be delegated to independent 'suspect hunters.'

13.14 A description of hunters and intermediaries

It would carry us too far to treat all possible variations on the tasks of, and on the distribution of tasks between, hunters and intermediaries. The foregoing explanation is deemed to have sufficiently illustrated the basic idea. Now this idea has been made clear, we will make an attempt to give a concise description of the notions of hunter and intermediary.

A *hunter* is an organization that manages at least a part of the means for transmitting and/or receiving being present in the outside world (i.e. being outside vehicles) for the sake of the communication between vehicles and the traffic information system or the rest of the traffic information system (or the authority or the rest of the authority, respectively) and that makes a contribution to keeping secret as much as possible the position of a person or a vehicle, in particular at the moment of reception of a message from that vehicle.

Primarily we allude here to the 'pure' hunter as described in the previous section. A 'pure' hunter keeps no accounts and forwards each received message to an intermediary, but only after both 1) having added to the message the date and time of reception, the location of reception and/or the location of the person or the vehicle at the moment of reception, and 2) having signed the thus resulting message. (If one is content with a weaker system, one can drop the last requirement, for example.) A 'pure' hunter can thus only function if there is also at least one intermediary. Carrying out certain counteractions, i.e. the task of 'suspect hunter' (see the previous section), can also be counted as one of the tasks of a 'pure' hunter.

Secondarily we use the term hunter also for a hunter that additionally performs – all or at least a part of – the tasks of an intermediary. (In other words, for a hunter that also acts as a 'whole' or 'semi' intermediary.)

An *intermediary* is an organization that is independent of the authority and that, for the benefit of the privacy protection, acts as a middleman for the communication from vehicles with the authority. An intermediary (more precisely, the first intermediary in a possible chain of intermediaries) separates the signature of the hunter and the data that have been added by the hunter (i.e. location and point in time) from the message and retains this for a certain time in a privacy protecting way. The rest of the incoming message is deciphered and forwarded to the next addressee, i.e. the final recipient or the next intermediary in the chain. If an intermediary receives a certain message other than as the first intermediary in the chain, then only the task sketched in the previous sentence need be performed on that message. Besides this, all intermediaries will, in one way or another, take care of making return messages possible.

13.15 Applications of the sketched approach for privacy protection

It would carry us too far to treat all possible variations exhaustively. On the basis of the approach described first and the variation with hunters and/or intermediaries just described, the basic ideas are deemed to have become

- 8 SEP 2003

sufficiently clear. For a person skilled in the art, this will be sufficient to be able to apply the protective measures against illegitimate tracing in a TIP system (thus including all kinds of variations falling under such a system).

We have shown how privacy can be protected, even if messages with an identification are continuously being transmitted from each vehicle. The said identification can be used not only for traffic pricing, but, if desired, for other applications as well, such as, for example, speed measurements at certain locations. In the next chapter we will first digress somewhat on the identification of persons and objects, or rather on the problems associated with the identification of persons and objects, before we will show, in Chapters 15 and 16, that the use of hunters and/or intermediaries can also be avoided.

In Chapter 15 we will show that, for a number of applications, semi-identification numbers can be used instead of identification numbers. The 'detour' via hunters and/or intermediaries is then no longer necessary for the protection of privacy. In Chapter 16, we will show that the use of identifications can be reduced even further, namely so far that the use of hunters and/or intermediaries is not or hardly necessary anymore. The use of agents and semi-identifications will therefore appear to be a very attractive option.

14 Identification

We have used the term identification already many times somewhat loosely, namely to denote an identifying datum or an identifying combination of data. Undoubtedly, we will do that still more often, although strictly speaking the term identification concerns – the process of – the ascertainment of the identity of a person or thing. In this chapter, we will enter into some details of the latter in particular.

14.1 Problems with the identification of vehicles

When registering a vehicle in the central license plate registration in the Netherlands at present, a registration certificate, consisting of a number of documents, will be issued. These official documents are liable to all sorts of fraud. Furthermore, not only these paper documents, but in particular also the corresponding vehicles are tampered with. According to news reports, driving with false license plates (which is alarmingly easy and for years has seemed to yield a too low probability of being caught), but also – the more difficult – tampering with identification numbers on chassis and engine (such as modifying, removing and/or re-creating) seem to happen all too often. Therefore, there is need for a more fraud-resistant way to couple registration numbers, chassis numbers and the like with vehicles.

One possible idea is to furnish the vehicle with a component that contains the chassis number (or the registration number) and that can make this number available to the outside world. However, making a *constant* bit pattern available may lead to undesired problems. After all, the disadvantage is that the bit pattern in question can be intercepted. (And that is all the more a real possibility if the bit pattern is sent via a transmitter.) Thus it is possible to make false components that do exactly the same as the original. In other words, the problem is that the recipient of the bit pattern cannot ascertain (remotely) the authenticity of the bit pattern and of its sender. In short, when using such components fraud, generally speaking, seems to be easy.

14.2 No interchange of constant data for identification

This objection against the use of – passive – components that make a constant bit pattern available, is somewhat comparable with the objection against the use of passwords or personal identification number (PIN) codes for

- 8 SEP 2003

securing the use of identification aids, such as PIN cards, that are applied for many systems, such as, for example, payment systems and automatic teller machines. The objection is in both cases that during normal use a constant datum must be interchanged and that this constant datum runs extra risk of being intercepted especially during this interchange. Think, for example, of interception by peeping at the keyboard without being perceived (for example, by using mirrors and/or a hidden video camera or by using an inconspicuous substance on the keys) or of eavesdropping the communication or telecommunication during the sending of the PIN code or the password. After interception a copy of the constant datum can be used as original, because for bit patterns there is no difference between original and copy.

14.3 The problem of fraud-resistant identification in general

Consequently, in general it is true that for good protection against fraud, – direct – interchange of crucial information should be avoided as much as possible. Therefore, it is better to prove – indirectly – that one possesses certain crucial information, without revealing that information itself[42]. This approach is known as using *challenges*, that is to say, challenges in which one must demonstrate a unique capability.

A good example of this approach is unique identification by means of putting a digital signature. One then demonstrates that one is capable of putting a signature on a certain message without revealing the bit pattern (i.e. the key) on which that signature is based[43].

Of course, the message on which the signature is to be put, should be usable only once (after all, copies are not allowed to have any value), and thus must be a new one each time again. Furthermore, it must be an absolutely harmless message, that is, signing it may not possibly lead to undesired consequences. For example, it may certainly not be so that by signing one enables the other party directly or indirectly to obtain a false signature on another message (e.g. a contract) with undesired consequences.

Without wanting to enter into details of all further difficulties, we give one suggestion for such 'harmless only-for-identification messages' and a corresponding identification protocol. To meet the requirement of uniqueness and inconstancy, we require that each such message contains the point in time concerned in a certain and fixed, prescribed format. To prevent somebody from using elsewhere and – almost – at the same time a copy of someone else's identification to falsely impersonate himself as that other person, each such message must also be specialized for the one identification process in question. This can be done, for example, by arranging that the identification questioner must always first send a signed identification request[44] that contains the time of that request, to the person or object to be identified, and that the to be identified object or person (at least, if he or she

---

[42] An alternative is to arrange that crucial information is no longer crucial immediately after the first interchange, i.e. to use a different bit pattern each time. One may thus still use passive memory means, such as, for example, a magnetic card. However, because it is easy to read, modify and write the bit pattern on, for example, a magnetic card, this alternative is still subject to various difficulties. Anyway, we will here not digress further on this alternative and its limitations.

[43] To skilled persons it will be clear that here we have in mind particularly the use of asymmetric cryptography, i.e. public key cryptography. The said key that is not revealed will then concern the private key.

[44] This also solves the problem of forgeries, such as, for example, counterfeited automatic teller machines.

-8 SEP 2003

wants to meet the identification request at all) then signs that identification request, preferably after itself, himself or herself respectively having added to it the point of time of signing.

For the rest we remark additionally that in certain cases it is possible to use identification means with a collective (or partly collective) signature. If the care for the supply and the correct working of the identification means is entrusted to a certain organization, it is for example possible to have several, and possibly even all, identification devices making use of the same 'basic signature'. The 'basic signature' then serves to prove that the identification device in question is original, i.e. is handed out by the thereto authorized organization.

Said organization then does have to arrange that each identification device possesses a unique identification number too, and that this unique number always will form part of each signature put on any identification request with the help of the 'basic signature', for example, by adding the unique number to the identification request to be signed before signing it. This unique identification number thus must always be used together with the 'basic signature' to form the complete, identifying signature. Consequently, it must be protected against theft just as well as the key of the 'basic signature'. In other words, the unique key on which the complete signature is based, consists in this case of both the unique identification number and the collective key used for the 'basic signature'.

All in all we hope that the above text has made sufficiently clear that for good identification one needs preferably some means being capable of performing the required processing, say, a small device that can put signatures. If each such a small device is sufficiently protected against theft of its key, i.e. of the key on which the digital signatures that can be put with it are based, then that small device is sufficiently protected against impersonating by a forged copy.

If we are capable of making small devices that can identify themselves uniquely and fraud-resistantly, we strictly speaking have not found a solution yet for the identification of arbitrary objects (also including persons). After all, to be able to use such devices for fraud-resistant identification of objects (persons inclusive), we still have to connect these in an adequate way with the objects in question as well. In the following two sections we will enter into somewhat more details of coupling identification devices with persons, respectively vehicles.

14.4 Personal identification

If we hand out to each person one unique and fraud-resistant identification device, we therewith do not – yet – attain that each owner of such a device can identify himself fraud-resistantly. After all, the identification device can, for example, be lost or stolen. So, among other things, care must be taken to ensure that the identification device cannot be used without permission of the rightful owner. The latter is sufficient in case of, for example, transfer of payments, but not for personal identification. For reliable personal identification the device must be associated fraud-resistantly with one correct person, which implies that it must even be prevented that the identification device can come to be used for or by another person with the assistance of the owner.

For both transfers of payment and personal identification, we have found solutions that offer much better security than the existing solutions known to us. Our solution is particularly suited for transfers of payment, because it does not only offer excellent protection against the risks mentioned earlier such as, for example, 'leakage' of the PIN code either by peeping or eavesdropping or by errors or fraud within the PIN code supplying organization), but also is very simple to use in practice. It thus meets the important requirement of practical usability for the general public. However, on second thoughts we have decided not to reveal the solution concerned in the current context, i.e. in this application for a patent on the TIP system.

-8 SEP 2003

14.5 Vehicle identification

Two sections back we have described how an identification device can uniquely identify itself. By attaching to each vehicle such an identification device, one already obtains a significantly more fraud-resistant way of identification than that of the current approach.

After all, it will then be prevented that the identification function can be taken over by a forgery. And there is no use in rendering the authentic identification device inoperative only, since the absence of a well-functioning identification device can be detected sufficiently easily (in particular during the use of the vehicle).

Thus, although the protection of the identification device against actual destruction or removal on itself is still equally difficult, one yet can arrange sufficiently that only rendering the original identification device inoperative by destruction or removal will not pay off at all, by imposing sanctions on the absence of a correct functioning identification device.

The only remaining fraud possibility against which protection is still required, thus seems to be the mutual interchange of authentic identification devices of a number of vehicles. Although the advantage that can be gained by interchange will be in many cases – already more – limited, one really has to defend (or arm) oneself against it in certain cases. The latter is the case if the identification and/or classification of the vehicle must be very fraud-resistant, i.e. also resistant against interchanges, for example because different rates are applicable to different vehicle types in case of traffic pricing.

Thereto, one possibility is to attach each identification device to the corresponding vehicle in such a way, that it is impossible, or almost impossible, to remove without causing fatal damage, i.e. without overriding the correct functioning of the identification device.

If vehicles are furnished with fraud-resistant identification devices, this offers a number of advantages. One advantage is that traffic offenses then can be settled more efficiently and more accurately. Due to the fully automatic identification, no license plates have to be recognized anymore, as currently is usual. Furthermore, certain problems resulting from the use of false – or, probably better formulated, misleading – license plates will vanish. To obtain these advantages, it is often not even necessary yet that the identification devices have been attached to the vehicles fraud-resistantly, because it can be avoided in other ways that interchanges will be profitable. (For more details regarding the latter, we refer to the example in Chapter 17.)

15 Semi-identification and its applications

Before proceeding with the treatment of an important variation, namely the approach using agents, we first introduce the notion of semi-identification and show some examples of purposes for which semi-identifications (or semi-identification numbers) can be used. One application concerns anonymous inspection (i.e. verification) of the precision of counters. Another application is, for example, privacy-friendly and automatic ascertainment of traffic delays, e.g. due to tailbacks.

15.1 The kilometer counter value as semi-identifying datum

For inspections on the proper maintaining of counter values, it is of essential interest that two messages that are received from a certain vehicle that passes two successive receivers, have a high probability of being recognized as being related to each other. Hereto one can add an identification number (of the vehicle or the vehicle equip-

-8 SEP 2003

ment or the like) to each transmitted message. The nice thing is that for the verification of certain counters, such as, for example, kilometer counters, addition of a unique identification is not strictly necessary. After all, the kilometer counter value of a vehicle may itself already be a, what we will call, semi-identifying datum with sufficient uniqueness. (Actually even with too much uniqueness, but we will come back to that later on.)

We will digress on the subject of semi-identification presently. But to improve the understanding of some things, we first explain that almost always one can recover the relationship between related kilometer counter values. After all, since the kilometer counter values of a not all too large number of vehicles in general will differ sufficiently from each other, two messages will very likely be related, i.e. originate from the same vehicle equipment, if the difference between the two kilometer counter values reported therein does not, or hardly, deviate from the length of the checking trajectory. (Note: The size of allowed deviations is not only determined by the required accuracy of the kilometer counter in the vehicle, but for example also by taking into account the effect of a fluctuating course of the vehicle, e.g. due to manifold changing of lanes. In short, the accuracy of the inspection plays an important role for the size of allowed deviations.)

If ever there are coincidentally several possibilities to pair messages, such as, for example, in case of two vehicles that shortly after each other enter the same inspection trap with – almost – the same kilometer counter value, then one has the choice of either 1) starting an action against the vehicles involved to have them be further inspected, or 2) just drop the vehicles involved from the scope of this inspection. As the probability that such a thing happens is sufficiently small, such escapes from one specific inspection will, in general, not pose a problem.

But in the case that such vehicles are kept outside the scope of the inspection, one has to avoid in some way or another systematic abuse of this possibility. Someone could try, for example, to escape from inspections during a certain period by making his vehicle represent itself continuously – during that period – as two vehicles with the same kilometer counter value. Such a situation can be detected and thus countermeasures can be taken. Here we are only concerned with mentioning that one must be alert for all kinds of fraud attempts.

Anyway, the underlying principle of *pairing*, i.e. finding out which kilometer counter values are related to each other, is now supposed to have become sufficiently clear to a reader skilled in the art to enable him (or her) to work out, or further work out, specific examples for himself (or herself) and to sufficiently understand the concise formulation below – or the underlying idea – of the notion of semi-identification (or semi-identification number) introduced by us. The manner of relating just described we occasionally call the *pairing trick*.

15.2 Semi-identification

With the term semi-identification we have introduced (in the meaning of semi-identifying datum[45]), we mean a datum[46] that is not unique and/or predictable enough to be able to uniquely represent the corresponding object (or person) through time within the set of all relevant objects (or persons respectively), but is sufficiently unique and

---

[45] The word semi-identification should perhaps be used only for the semi-identification process. Thus, we use it, just like the word identification, somewhat loosely. (See our earlier remark about that at the beginning of Chapter 14.)

[46] Or a combination of data.

-8 SEP 2003

predictable to offer a sufficiently high probability of being able to represent the corresponding object (or person respectively) uniquely within a relatively short period or in a relatively small subset of all relevant objects.

In our example the kilometer counter values were sufficiently unique to be able to distinguish almost all vehicles that pass the respective start or end of a checking trajectory in a certain limited period from each other with high probability and in addition were sufficiently predictable – at least within the checking trajectory in question – to be able to recover almost all related pairs. In this example, the size of the period in question is roughly limited by the maximum time required by one of the vehicles in question to travel the checking trajectory.

However, kilometer counter values are not yet good enough for practical use as privacy-protecting semi-identification number, since for kilometer counter values it roughly holds that the higher the value is, the more selective it will be, i.e. the more it will approximate a unique identification. Besides, the total number of participating vehicles does also play a role for the degree of uniqueness, just as the smallest distance unit indicated by the kilometer counter does. All this together makes that kilometer counter values, and particularly high ones, often will have a too high uniqueness for our purposes, or will even be uniquely identifying instead of semi-identifying.

Note, however, that this is not a problem at all for the inspections just sketched as such, but should be seen as a problem if we take the desire for privacy protection into consideration. In extenuation it should be remarked, though, that kilometer counter values still are much safer for privacy than registration numbers or other vehicle identification numbers, as kilometer counter values change continually and the changes between two observations are not – always – fully predictable. Anyway, we will explain how one can get better semi-identifications.

15.3 Artificial semi-identification numbers

One can also create an artificial datum that is suited for use as semi-identification or semi-identification number. Namely, in particular by making for each vehicle a random once-only choice from a set with a suitable number of distinct elements and then using that chosen element as permanent semi-identification for that vehicle. Thus, one can, for example, choose for each vehicle once-only a random number from a limited range and then use that number as permanent semi-identification number.

Suppose that for each vehicle a four-digit random number is chosen. Then, in the case of a total number of, for example, 5 million vehicles, each semi-identification number will be used by 500 vehicles on the average. (Note: From the viewpoint of privacy protection this is, by the way, still somewhat little.) However, within a random subset of, say, 1000 vehicles the far majority[47] of the vehicles then really will be uniquely identified by their semi-identification number. So, as long as there are, in this example, at every moment less than, say, 1000 vehicles within an inspection trap, such an artificially generated datum can be used very well to 'identify' related kilometer counter values.

Despite this local 'identification', privacy then still is protected to a certain extent, because the vehicle in question cannot be fully tracked in the traffic. After all, even in case of a rather dense network of receivers along the roads, full tracing remains almost impossible, for example because of the probability of 'encounters' with other

---

[47] For a precise computation we refer to the 'birthday problem,' well-known in mathematics, which is closely related to this.

-8 SEP 2003

vehicles with the same semi-identification number. By the way, note that something similar is true if one would use for the semi-identification a part of the vehicle registration number, such as, for example, the last three or four digits and/or characters.

In case of this kind of semi-identification numbers the degree of privacy protection depends, for example, on: 1) the size of the set from which the semi-identifications are chosen randomly, 2) the total number of vehicles in the area in question, 3) the size of the area in question, and 4) the intensity by which the vehicles in question are used. In short, it is not always very easy to choose a suitable (i.e. not too large and not too small) range of numbers.

15.4 Semi-identification numbers based on a counter value

The approach just explained can simply be combined with the use of sufficiently predictable counter values – such as, for example, kilometer counter values – which leads to a considerable improvement with respect to separate use of one of both methods. Hereto one can simply choose a part of the digits, say four, from the counter value. For example, if the kilometer counter value is correct to at least one decimal, one may choose for the rightmost three digits to the left and the leftmost digit to the right of the decimal point of the kilometer counter value.

For the selection of a range or sub-range, it is not strictly necessary to choose a number of digits from the counter value, but it is also possible to use all sorts of computations, such as, for example, computations involving a modulo operator and/or a division operator with rounding to the nearest smaller integer. In the rest of this text semi-identification numbers usually are supposed to be of the type based on a – verifiable or sufficiently predictable – counter value.

15.5 Verifications of counters with the aid of semi-identifications

As was already indicated at the beginning of this chapter, the type of semi-identification numbers just mentioned can be used for checking whether counter values are kept correctly. Not only for verifications of the counter used for the semi-identification number, but of course also for those of other counters. It may surprise some that counter values can be used for the verification of counter values, but it is really so. Although now it actually should be clear already how this works, for clarity we give an explicit explanation anyway.

For the verification of the precision of an arbitrary counter, the last so many digits (i.e. a generally small number of the least significant digits) of the counter value to be verified should be transmitted continually from the vehicle together with the vehicle's semi-identification number. (Thus, if the so many digits are also used as semi-identification, then only the semi-identification number has to be transmitted to be able to verify the precision of the counter on which the semi-identification is based.) Verifications then can be performed by intercepting on two points that will be passed by successively, the corresponding transmitted messages. With aid of the pairing trick, one then can determine for each vehicle how much its counter value has been increased (or decreased) between the beginning and the end of the checking trajectory. Assuming that one externally (i.e. in the outside world) ascertains or has ascertained how much the counter to be verified should change, one can compare the correct, required change with the change between the two counter values that have been made available from the vehicle.

-8 SEP 2003

For example, if the semi-identification numbers exist of the last four digits of kilometer counters with one decimal, i.e. kilometer counters indicating hectometers, then only these semi-identification numbers have to be transmitted and then the precision of the kilometer counters can be verified by intercepting the semi-identification numbers in question on two points along the road with a known distance between them.

In short, for the verification of the precision of kilometer counters and other counters real identifications are not necessary, and semi-identifications (or semi-identification numbers) can be used to make the protection of privacy easier. However, note that with the approach described until now (with remote verifications only), real identifications still have to be used as well, because they are required for the verifications on the monotony of counters.

15.6 Fully automatic ascertainment of traffic delays

The pairing trick in which part of a sufficiently predictable counter (or counter value) is used for semi-identification, can also be used for other purposes. Based on the above, it will be clear that for vehicles that pass both receivers, the time they required for the trajectory between the two receivers generally can be ascertained precisely by means of semi-identification.

If on the basis of a sufficient number of such vehicles one computes the average of the traveling times realized on the trajectory (and thereby possibly leaves out of consideration all too far deviating values), one can subtract from this actual average traveling time the average time usually required for this trajectory if there are no tailbacks, and thus ascertain the actual traffic delay precise to the minute. In short, the transmitted semi-identification numbers can be used for continually and fully automatically measuring the traffic delays in a privacy-friendly manner.

For the rest we supplementarily remark that traffic delays expressed in time (say, minutes) often offer much better information than the length of tailbacks expressed in distance (say, kilometers). After all, a tailback of one kilometer at an average driving speed of 5 km/h results in more delay than a tailback of five kilometers at an average speed of 30 km/h.

15.7 Trajectory speed checks

Of course the pairing trick can be used for still more applications, such as, for example, for performing trajectory speed checks in a very easy and privacy-friendly way. In the case of a trajectory speed check, one ascertains for each vehicle that travels a certain trajectory with known length (or for each person in that vehicle), how much time elapses between the passing of the beginning and of the end of the trajectory. In this way one can determine for each individual vehicle the average speed with which that individual vehicle has traveled that trajectory.

15.8 Possibly integrated traffic fines

Now we are discussing speed checks anyway, we here take the opportunity of just glancing at the possibility of perhaps integrating the 'price' of speeding in the tariff function used for road traffic pricing instead of imposing separate fines. If so, then automatically an extra high price will be charged for each distance unit that has been traveled with a speed higher than the locally valid speed limit. Of course, such integrated traffic fines, that is, traffic fines integrated in the tariff, cannot only be applied for speeding, but also for other offenses, such as, for example, producing too much noise.

-8 SEP 2003

In case of this last example, think particularly also of application in the context of air traffic. One might use fines (integrated or not) to limit the noise nuisance by aircraft. One plausible approach is to take the nuisance observed on the ground as starting point and thus to allow an airplane to produce more noise at higher than at lower height. Undoubtedly, the function for determining the allowed noise production then will not only be made dependent of the height, but for example also of the distance to and preferably even of the position relative to the airport[48], so that take-offs, landings and prescribed approach and fly-out routes can be taken into account.

For the sake of clarity, we emphasize that the imposition of traffic fines (whether integrated or not[49]) is a possible TIP system application being separate (independent) from using semi-identifications or not. The reader should therefore not be misled by the fact that we have raised the matter of integrated fines in this chapter incidentally and just for a moment. (By the way, we do make such side-notes, i.e. jumps aside, more often in this text. Usually even without mentioning explicitly that we jump aside.)

15.9 The benefit of semi-identification

We have shown already in Chapter 13 that privacy can be protected with some effort (viz., by using hunters and/or intermediaries), even if real identification or real identifications are used. However, it is simpler, and thus also less expensive, to apply semi-identification or semi-identifications where possible. The privacy then is sufficiently warranted, while the manager of the infrastructure (say, government) then still can obtain direct access to certain required or desired information. After all, all examples given in the introduction for traffic management and control can be implemented in a privacy-friendly manner by means of semi-identifications.

We take as example an integrated traffic information system for traffic pricing and traffic control, in which the vehicles receive messages (about speed limits, tailbacks, traffic delays, and the like) and transmit messages themselves. Say, transmit themselves messages with semi-identifications in them for the benefit of speed checks and traffic control, and messages containing identifications for the benefit of traffic pricing. In this example, the traffic manager (say, the government) then can derive the necessary information from the directly accessible semi-identifications, while only the messages containing identifications require a roundabout route (at least in the case of the approach described up to now using hunters and/or intermediaries) on their way to the intended recipient (i.e. the government).

We will show in the next chapter that the privacy threats due to the use of identifications can be reduced further by means of agents, and indeed so much that the use of hunters and/or intermediaries is not, or is hardly, necessary anymore. It will appear to be a very attractive option to use both agents and semi-identifications.

16 An approach using agents

It is unfeasible to explicitly describe all possible variations of the TIP system. Yet, to make clear which possibilities exist for the implementation of the TIP system, an example is given in this chapter in which two aspects which were previously mentioned but not explained in detail, play a role. These two aspects concern the trans-

---

[48] Note that the geographical position of a commercial aircraft is not usually considered to be privacy-sensitive.

[49] Probably it is usually wiser not to integrate fines into the tariff, but to register them separately.

mittal on demand only and the use of a fraud-resistant component. On the basis of this example these two aspects should become more clear.

16.1 Transmitting on demand only

If messages with the required data are not transmitted continuously, verification becomes considerably more difficult. After all, knowledge of the moments when data has to be provided to the inspector creates a broader opportunity for fraud. This is best illustrated by means of an example.

Suppose that at a certain moment at location X the kilometer counter value of a particular vehicle has been given. If the next request – or, better stated, the next order – reaches said vehicle at location Y, then the kilometer counter value should have been increased with at least the length of the shortest possible route from X to Y. As long as this principle is not violated, the inspector will not be able to find anything objectionable. This means that if a larger distance has been covered, for example because in the time between these two checks also location Z far from the route between X and Y has been visited, the distance extra covered (or a part of it) can be concealed.

One possibility of counteracting this is to increase the density of the network of checkpoints, and thus the frequency of issuing orders to transmit data, such that this form of fraud will not be worthwhile any longer. This option seems rather unattractive because of the associated costs.

16.2 Use of agents

Another, much more attractive possibility is to have – a part of – the check performed in the vehicle by, what we have called, an agent. On the one hand, an agent has to offer specific certainties to the data collecting and/or verifying authority, and on the other hand the agent should not be able to breach the desired privacy. As stated earlier, an agent consists of software and/or hardware that is trusted by – at least – the authority.

In the following we will leave open as much as possible whether an agent is implemented as fixed [alternative translation: permanent] or as loose [alternative translation: removable] vehicle equipment, but both are possible, even at the same time! (At the end of this chapter we will say more about this.) Also we will dwell as little as possible on details of all kinds of other variations, for example those that are a consequence of each agent being uniquely identifiable or not, or of possibly distributing identifiable agents in an anonymous or semi-anonymous way. Nevertheless it will become clear to a reader skilled in the art that, if the agent consists of a chipcard, our example can also be seen as a further illustration of the possible use of chipcards that are, or are not, anonymous or are, or are not, anonymously or semi-anonymously delivered, as has been suggested earlier in this text. (See Chapter 13.)

In general, an agent maintains, in a vehicle participating in traffic, supervision on certain matters. Upon authorized request (and/or now and then on its own initiative), the agent provides a personally signed report on its findings. Such a report can then be transmitted via a transmitter to the authority (e.g. the authority managing the traffic information system or a separate authority supervising the agents).

The transmitter and/or receiver do not need to be trusted by the agent and/or the concerning authority. To simplify our explanation, we will assume that the transmitter and the receiver are not part of the agent. Of course, committing fraud unnoticed by obstructing the communication will be made impossible. This can be done by the use of explicit or implicit acknowledgements, i.e. of confirmations of receipt. If, for example, a request for a report by the agent is made, it is the task of the other vehicle equipment to provide an adequate response. Be-

-8 SEP 2003

cause the aforementioned report is necessary for an adequate response, the agent needs to be involved and the transmission of the report cannot be prevented unnoticed. In this example, explicit acknowledgements thus are not necessary.

The report, made and signed by the agent, is – preferably – always first handed over to the other vehicle equipment. After all, the owner and/or user of the vehicle does/do not have to trust the correctness and integrity of the agent. Before transmitting the report of the agent, the vehicle equipment can, among other things, verify whether the agent has indeed adhered to the precisely prescribed data and formatting of the report. It can thus be avoided that the agent surreptitiously includes illicit, privacy-sensitive information in his report or that the agent abuses the transmitter for sending messages to the authority illicitly often, which can endanger privacy. The correctness of the agent can also be doubted. If that is the case, then, besides the report, an annotation also needs to be included in the response to be supplied.

When all checks have been made and the response to be issued (consisting of the report of the agent and possible annotations) has been composed and signed, the signed response must be handed to the verifying authority via the transmitter. It can be agreed upon that the verifying authority must return a receipt upon receiving an adequate response. If the response included an annotation of disagreement or of doubt regarding the correctness of the report by the agent, then, within a certain period, an agreed procedure will be followed, such as offering the vehicle together with the agent for further inspection and verification.

16.3 Supervision by the agent on counter monotony

As sketched before, the agent has in any case the task to provide, if required, a signed report on his findings during supervision. Among other things, an agent can supervise that it is continuously informed, at least during driving, on the values of one or more counters or about the increases thereof. Thus, the agent can verify on the spot the monotony of one or more counters or use the given data to update one or more counters itself such that these are monotonically increasing. Both these cases amount to the same thing, but for convenience we will assume that only increases (pulses or otherwise) are provided, and that the agent updates the counter value (or the counter values) itself. Note that when using an agent *no* identification of the vehicle is required for the verification of the monotony of counter values; identifications *were* necessary in the case of remote verification.

16.4 A contribution by the agent to the verification of counter precision

The agent can, and in general should, also supervise that the counter value is not increased too quickly. Thus, a sudden increase with too large a distance is not allowed. Stated differently, an increase that corresponds to an excessively high speed[50] does not have to be believed and possibly neither will an all too sudden increase in speed, i.e. an impossibly high acceleration. In this way, the form of fraud sketched in Section 16.1 can be combated. This will be explained now.

Suppose the agent reported at location X a certain counter value. Then the agent can be misled by not passing counter increases during driving and thus one can pretend towards the agent that one is not driving. Or one can pass too low or too few increases. But, such a deceit will be revealed as soon as a request for a response comes

---

[50] For example, higher than the maximum speed attainable with that vehicle, taking into account a certain margin in view of special circumstances.

in, say, when passing by location Y. After all, one then cannot succeed anymore in making the agent as yet sufficiently increase his counter value in a short time, in order that at least the shortest distance between X and Y is included in his counter value. Therefore, the counter value of the agent then possibly will be too low and the fraud will be revealed after transmission of his report. The only alternative is to not give an adequate response, but that means that it will still be detected that something is going on and that action can be taken. In short, since every agent maintains the counter value itself and since it only does so on the basis of limited increases, such fraud with counter values will not be possible or will not pay anymore.

We now have discussed how an agent can guarantee monotony and that an agent can and may have to detect implausible increases of the counter value. If anything seems to proceed incorrectly, the agent has to report on that at some point in time, for example as soon as it gets an opportunity to do so. Not accepting too implausible increases is necessary as a contribution to the verification of precision.

If the agent does not do more than described so far, the remainder of the verification of the precision of the counter has to be performed by the verifying authority. However, an agent may perform even more verifications. In the following, we will show that an agent can also perform the remaining verifications of precision itself.

16.5 Complete verification of counter precision by the agent

For an agent to be able to verify the precision on its own, i.e. to be able to verify whether the other vehicle equipment constantly keeps it correctly informed about the correct increases of the counter value, it does need to have reliable information available now and then.

We will now illustrate one thing and another for the case of kilometer counters. In this case, the agent must now and then receive reliable information on the correct speed or about the correct length of a specific traveled trajectory. This might be achieved, for example, by the agent itself being able to determine its geographical position, or by the agent occasionally receiving information sent to it on its position or on the position of the vehicle it resides in. As we now will show first, the latter might also be realized in such a manner that the agent does not even learn its position.

16.6 Kilometer counter verification based on positions that are (semi-)anonymous or not

The verification of the precision of kilometer counters can, for example, be realized as follows. At certain locations, imaginary measurement lines are drawn across the road. In the simplest case this concerns pairs of measurement lines, the first measurement line marking the start of a verification and the second one marking the end.

When an agent passes the first measurement line, a secret and signed message, containing both a timestamp and the message that a kilometer counter verification is started here, is sent to it. When passing the second measurement line, the agent again receives a secret and signed message, but now containing both a timestamp and the distance to the first measurement line. On the basis of the information supplied to it, the agent can determine whether the information on the kilometer counter values, supplied to it on this measurement trajectory from the vehicle, was correct.

The messages to the agent must be secret, because in this approach it is important for fraud resistance that only the agent is allowed to know where verifications begin and end. Therefore, in this case it will be also wise to use not only pairs of measurement lines, but possibly also verification trajectories with three or more measurement

lines. The latter ensures, for example, that the risk of being caught for fraud or a fraud attempt by means of 'smart gambling' on correctly guessed begin and end points of verification trajectories, increases considerably.

The signing of a message is necessary to prevent tampering (e.g. via manipulation with the rest of the vehicle equipment) with these messages, i.e. to prevent that messages can be forged or modified unnoticed.

To prevent messages from being delayed or possibly even not being passed on to the agent at all, it is possible to require that a confirmation of receipt, signed by the agent, must be returned in response. The timestamps help to prevent fraud by means of copied messages. Note that in this case, during counter verifications there is in a certain sense – still – a question of 'orders/requests' with corresponding responses.

In case of the above-mentioned verifications, one can make profitable use of semi-identifications. When passing each measurement line, an agent then gets a 'position message' sent to him containing some semi-identification of this measurement line (e.g. in the form of a two-digit number) and also the semi-identification or semi-identifications of one or more measurement lines that possibly have been passed by him earlier, together with their shortest distance to this measurement line.

One advantage of this alternative approach is that there is no longer any distinction between begin and end points of verifications and that the messages to the agents thus no longer need to be kept secret. Another, closely connected advantage is that the same messages now might be used in the vehicle for further determining the geographical position, for example in support of – possibly automated – navigation.

Note, however, that, if at each measurement line the broadcasted 'position message' only contains a semi-identification of the location, the agent does not get to know where it is and thus cannot give information to the rest of the supervising authority (or others) on its geographical position, not even via some covert channel[51]. But, for example, the driver of the vehicle may indeed already know his approximate position and, if so, use the semi-identification of the measurement line to determine now his precise geographical position, at least if this measurement line in question is at a known and fixed location.

For good verification, it is of course necessary that not all the positions of all measurement lines are known. For the required 'verifications by surprise' one may, among other things, use mobile measurement lines, i.e. mobile equipment for 'drawing' a measurement line and for transmitting the 'position messages' in relation to this measurement line. To be quite on the safe side, we finally yet remark that it is self-evidently also possible to supply in the mentioned – position – messages the distance to the measurement line in question instead of only the exact crossing of that measurement line.

16.7 Kilometer counter verification by means of reliable information on speed

Covered distance and speed are related to each other. If one is informed about the increase of the kilometer counter value and one has at one's disposal sufficiently precise time measurement, then one can determine the corresponding speed. But 'the inverse' is true as well, that is, on the basis of reliable speed data and precise time

---

[51] If one does not want to protect oneself against this possibility, then the positions of the measurement lines may also be denoted by unique identifications. The agent can then indeed come to know his position, but cannot just transmit this knowledge via the transmitter in the vehicle without a reasonable chance of being detected.

measurement one can verify the correctness of reported counter increases. In short, an alternative approach for verification makes use of speed data.

For example, one may ascertain the speed of passing vehicles independently by means of radar. The verification now can proceed in two ways. Either the externally determined speed is revealed to the agent and the agent verifies whether the speed based on the information supplied from the vehicle is indeed correct, or the agent transmits the internally determined speed and the verification takes place outside the vehicle.

Self-evidently, the two compared speeds should concern the same point in time. To be quite on the safe side, we here also draw attention to a fairly subtle point, namely that this should be a point in time before the moment at which a person in the vehicle can begin to have any reasonable ground to suspect that there is an increased chance of a check taking place soon. That is, a point in time before the start of any communication whatsoever with respect to this verification between the vehicle and the infrastructure. After all, to hinder fraud no information at all should be revealed on the basis whereof one might get any further suspicion of this point in time. In this approach to verifications, the agent should therefore always retain recent information on speed for a short time.

Of course the compared speeds should also concern the same vehicle. For more information on this, we refer to Section 11.4.

If the equipment needed for independent speed measurement is more expensive than an additional transmitter, then the approach of verifications by means of speed data may, in general, be less attractive than the one using position data. But even if so, this approach may then still be more advantageous for mobile checkpoints for the sake of verifications by surprise. Furthermore, this approach offers the possibility of verifications from moving patrol cars. In short, this approach is certainly interesting for mobile verifications in both meanings, i.e. movable and moving.

The example given in this section can be considered as a specific illustration of the earlier-mentioned, more general possibility to perform verifications using difference quotients or derivatives (differential quotients). (See also Chapter 11. We use the somewhat cautious formulation 'can be considered as', because, in case of external speed measurement, the speed is usually determined 'directly' by using radar waves and the Doppler effect, and thus is not explicitly determined as a derived quantity of covered distance, i.e. is not measured explicitly as a *difference* in distance traveled in a very short time.)

16.8 Other verifications by agents also

We just have described that maintaining the kilometer counter value and verifying its correctness can be done entirely by the agent if sufficient appropriate and reliable information is sent to it. As has been suggested before and should be clear by now, an agent can also check all kinds of other counter values and data, such as, for example, the engine speed, fuel consumption and/or noise produced in the engine compartment of the vehicle.

In the preceding section we have already described that an agent can verify the precision of the speedometer. However, since the agent is located in the vehicle and therefore can almost continuously exercise close supervi-

-8 SEP 2003

sion, it can also establish whether the locally valid speed limit is exceeded, at least if reliable information concerning the correct speed limit is sent to it from the outside world[52].

The agent may play a role in case of other traffic offenses also, such as, for example, driving through a red traffic light. For example, by revealing, upon authorized request, the identity of the vehicle or of the payer, at least if it has this information at its disposal. Or by establishing the violation in cooperation with the traffic light installation and recording this ascertainment.

When establishing a traffic offense, an agent has a number of possibilities. It can pass on the offense in due time to the rest of the traffic information system for further settlement, or it can determine the indebted fine itself and possibly add it to the already indebted amount of traffic fees. If the fine in question has been integrated, i.e. has been included in the tariff structure of the traffic fee, then it does not even have to do anything exceptional. This possibility exists, for example, for speed offenses. The fine may then be included in the tariff structure in such a way that the additional fine actually charged depends on the extent to which the speed limit was exceeded and on the number of distance units in which that happened. Of course, this dependency can also be arranged without integrating fines in the tariffs.

Anyway, fully automatic and efficient settlement of traffic offenses and fines becomes possible in many cases. If the agent takes care of making a fraud-resistant identification available, then traffic offenses can be settled much more efficiently, since reading vehicle registration numbers from, for example, photographs is then no longer necessary. In certain cases, such images can even be completely omitted, which yields considerable savings as well.

Finally we additionally remark that the settlement of fines is fairly well comparable to imposing and collecting open tolls, such as, for example, in the case of open tolling at bridges or tunnels. Up to now, we have hardly paid any attention to the latter, among other things because open tolling is much more common than continuous pricing. Although the use of a TIP system solely for open tolling is perhaps somewhat less remarkable, it may be clear that our approach also offers certain advantages when used for open tolling.

16.9 Privacy protection by reducing the transmission of identifications

If the agent takes as much responsibility as possible upon itself for all verifications, then hardly any other messages need to be transmitted by it than the messages for acknowledging the receipt of reliable information transmitted to it, such as, for example, position data, externally measured speed, noise and so on. The only things that need to be transmitted additionally are reports by the agent on the course of affairs – whether correct or not –

---

[52] In general, one will not appreciate continuous supervision of one's behavior in traffic (Big Brother). However, such comprehensive surveillance by an agent in the vehicle may possibly be quite acceptable if, on the contrary, it restricts itself to a judgement of the quality, or of the average quality, of the total behavior in traffic; in other words, if occasional violations are allowed to a sufficient extent. (Slight sloppiness, oversights and even some deliberate, deemed necessary violations then do not have to be fatal immediately.) Compare this, for example, to the better acceptance by traffic participants of sanctions for speeding if that offence has been detected by a trajectory speed trap than if it has been detected by the more usual speed trap, where speed is measured only at one specific spot.

and, in case of traffic pricing, now and then, say once per month, a report containing the relevant counter value and an identification number whereby a responsible payer can be identified indirectly. The latter is needed for the automatic collection of traffic fees. Perhaps very occasionally also a small number of messages will be exchanged additionally, for example because it is deemed necessary to occasionally perform an – additional – remote verification on the correct functioning of the agent.

Strictly speaking, an agent does not, of course, per se have to supply the reports on counter values and correct or incorrect functioning: 1) automatically, 2) as soon as possible, and/or 3) during driving. In principle it is also possible, for example, to have the agent periodically be 'read out' by or on behalf of the authority. This reading out, i.e. this requesting and obtaining a report, does not have to take place via the transmitter of the vehicle, but may also take place via physical – e.g. electrical – contact. The reading out might, for example, be combined with – possibly other – periodical tests and inspections. Even if reading out were to take place once a year only, the payment may of course be spread as well (or equally well), just as currently is usual in The Netherlands for payment of, for example, natural gas and electricity.

Nevertheless we expect that one mostly will choose for reading out via the transmitter of the vehicle during normal use because of the advantages offered. After all, it does not cost the customer any time and one may therefore, without too many objections, also read out the agent more often. Moreover, fraud or fraud attempts (and incorrect functioning more in general) then are revealed earlier, so that action can be taken sooner.

If the agents are not uniquely identifiable, i.e. if they do not each have their own signature, or if the agents really are uniquely identifiable, but it is not known by which person or in which vehicle an agent is used, i.e. if agents are delivered anonymously, then the confirmation of receipts signed by the agents do not reveal any privacy-sensitive information. Thus, the only messages that still might threaten privacy are then the reports on the counter values with the accompanying identifications for the benefit of the payment process. If these latter messages are transmitted only occasionally, for example once per month, there is hardly any threat to the privacy, not even if one could precisely ascertain for each such a counter value report from where that message was transmitted. (For such messages one could possibly use a communication channel for which the sender is not readily locatable.)

Something similar to what has been described above holds when the agents are identifiable, but are delivered semi-anonymously. In short, the privacy protection by means of hunters and/or intermediaries can, in the cases mentioned, be omitted partly or possibly even completely! Possibly one could also have the payment take place within the vehicle. Somewhat more will be said about this in the next section.

16.10 Differences with the approach discussed earlier

The approach using agents does not actually differ much from the approach with remote verifications only that was discussed earlier. One difference is that the verifying authority, via advanced posts – namely agents – is closer to the objects to be monitored and that verifications (all verifications or possibly only a part thereof) occur in the vehicle. The communication between the – often not fraud-protected – objects (in particular, for example, sensors and/or measuring instruments) in the vehicle and the information collecting and/or verifying authority now occurs mainly or completely within the vehicle (namely, between object and agent), so that for this communication it is no longer necessary to continually bridge the somewhat larger distances between the transmitter of the vehicle and the receivers in the outside world, or between the receiver of the vehicle and the transmitters in the outside world respectively. Thus, the communication channel between vehicle and outside world is no longer

– directly – used for the communication between the monitored objects (say, measuring instruments) in the vehicle and the inspector in the outside world, but instead is used now for the communication between the agent (as advanced post and possibly as full-fledged inspector) and the rest of the information collecting and/or verifying authority.

One thing and another is illustrated in Figures 3 and 4. In both these figures, the transceiver rendered on the right side relates to the hunter (represented by box 8) and there is in both cases one intermediary (box 9), although the latter is probably not, or hardly, necessary anymore in the situation depicted in Figure 4. In Figure 3, the authority, i.e. the final recipient (boxes 10 and 11), takes care of both the verifications (box 10) and the remainder of its tasks (box 11), such as, for example, collecting the indebted fees. In Figure 4, the verification tasks are performed on behalf of the authority by the agent in the vehicle.

One difference is thus that – at least a part of – the checking has been 'shifted', i.e. occurs at a different position in the total chain of activities and/or participants. This – in abstraction not so large – difference does really have essential consequences. After all, because the actual inspector itself is now located within the vehicle, there is no identification needed anymore to be able to determine whether different messages to the inspector (containing, for example, increases of counter values or other measurements) are originating from the same vehicle or not. Indeed, hardly any messages about monitored objects (measuring instruments) containing identifications of those objects still have to be exchanged with the outside world. As has been stated before, there still is only the need to occasionally send to the authority in the outside world a – possibly indirect – identification in a message with the resulting bill. And even this latter is not strictly necessary, because the agent can also be 'read out' during periodical inspections.

Even if the payment occurs inside the vehicle, the communication with the outside world does not necessarily have to encompass messages to the authority concerning the payments. But that communication will then, in general, be extended instead by an exchange of messages for the sake of the payment process. This last-mentioned exchange of messages concerns the communication between a bank agent, i.e. software and hardware of or on behalf of the bank, in the vehicle and – the rest of – the bank organization in the outside world. Do note that in the extreme case that agents only send messages to the outside world, i.e. to the authority, in the style of 'everything, including payment, is proceeding well', the authority (say, the fee collector) has no, or a less good, overview. This latter aspect may not be appreciated.

Another difference is that the required protection of the agent against fraud introduces a physical aspect. If the agent, for example, is implemented (realized) with the aid of a chip or chipcard, the total security depends on the physical protection of – the storage of – the software and the key or keys of the agent in the chip. Since in practice chipcards prove to be sufficiently protectable, and since no further physical protection is required, this does not seem to be a serious drawback.

16.11 'Fixed' or 'loose' agents

The use of agents seems an attractive possibility for carrying out tasks, such as in particular the charging of all kinds of traffic fees, and for performing the verifications required thereto. The agents in question can, for example, be installed in each vehicle as fixed vehicle equipment (FVE); say, in the form of a chip with software in some encasement. But an agent may, as has often been suggested before, also be implemented as loose vehicle equipment (LVE); for example, in the form of a chipcard that, at least during use, will be connected with the

-8 SEP 2003

other vehicle equipment of the vehicle concerned (such as, for example, the transmitter, the receiver, the battery and a number of sensors and/or measuring instruments) via a connection point (e.g. a plug or a card reader).

If every user has his own 'loose' agent, for example on a chipcard (which possibly also acts as identification device and/or consumption pass), and connects this card via a card reader in the concerning vehicle to the other vehicle equipment in that vehicle before each drive, then such an agent is of course not very suitable for the task of vehicle identification. In such a case a second, fixed agent can, if desired, take care of the fraud-resistant identification and/or classification of the vehicle. (See also Section 16.14.)

16.12 General and specialized agents

Sometimes we make for our convenience a distinction between general and specialized agents. With the term *specialized* agent we then allude to an agent with a specific function that is limited to only a small part of all agent tasks belonging to the traffic information system in question. Think, for example, of a fraud-resistant consumption pass that maintains a counter that is *essential* for the traffic information system and further performs no other agent tasks related to the traffic information system in question. (We refer to a counter as being only *informative* if it is only used for the satisfaction of the user and is not of decisive importance for maintaining the correct counter values by the traffic information system.) Another example is an agent that exclusively serves for the fraud-resistant identification and/or classification of a vehicle. On the other hand, a *general* agent performs all (or almost all) agent tasks that relate to the traffic information system in question.

Up to now, the term agent was mainly used in the text for general agents, and when reading the term agent one should (or was allowed to) primarily think of the pivot in the vehicle on which everything in relation to verifications in the vehicle hinges. Stated differently, the emphasis has always been on the verification task of the agent in particular, i.e. on its task as representative of the authority in a vehicle who takes care of – a part of the – verifications on the reliability of the information supplied in the vehicle and via which information is delivered to the rest of the traffic information system. In the rest of the text also, the word agent will primarily denote a general agent. Only occasionally we will additionally use for our convenience the term specialized agent. The difference between both terms thus plays hardly a role of significance. Rightly so, as the difference is indeed somewhat vague.

16.13 A little more on implementation possibilities

Just as in the approach with exclusively remote verifications, there are numerous – often obvious – implementations and/or variations possible when using agents. Therefore, it is too much of a good thing to explicitly enumerate all possibilities. On the basis of the given description, a person skilled in the art can easily conceive all kinds of different variations and implementations. Here we simply – and actually profusely – indicate only a small number of possibilities.

One obvious possibility, already often suggested before, is to implement the agents (i.e. each agent) as a chip, possibly installed in a chipkey or on a chipcard. Certainly if, for example, chipcards or chipkeys are used, one can also, if desired, provide the chips to be issued with a – say, decremental – counter, that consumption counter being maintained by the agent starting from a certain initial state. Thus, the agent then also takes care of the function of consumption pass, where the consumption of the credit balance can occur distributively over any number of different vehicles. The advantage of such an agent with consumption pass function is that tracing of

identifiable users of such chipcards is then impossible, simply because there are then no longer any user identifications in play. By restricting the sale of such chipcards, one can obtain, if desired, a system with tradable usage and/or pollution rights (per person per year).

We further mention the possibility of combining all mentioned functionality, possibly on one chip, with other applications, such as, for example, electronic transfers of payment with the aid of a chipcard or electronic access control with the aid of a chipkey. Indeed it then may be desirable to incorporate good guarantees against undesirable information exchange between the various applications. We also point out yet the possibility of extending the functionality of an agent. For example, to that of a '*reliable* black box', i.e. a black box that does not only register supplied data and retain these data during a certain time (as is usual), but in particular also *verifies* the supplied data (or a part of the supplied data) on reliability. Other examples are the possible use of an agent as a *reliable* taximeter or tachograph.

16.14 One or several agents per vehicle

Up to now we have kept, for our convenience, the possibility of several agents per vehicle outside of the discussion as much as possible. This was justifiable, so far as we are concerned, for a number of reasons. First of all, it did help to prevent unnecessary complexity of the explanation. Moreover, we have already explicitly mentioned in Chapter 5 that we wanted to abstract from the possibility of distributing processing over multiple processors, so that in fact we have indeed covered this possibility. The only special case that now will be discussed is the possible distribution of the agent's work over a 'fixed' and a 'loose' processor, i.e. a fixed and a loose agent.

In the case of a fixed agent, we often assume that it performs all desired tasks. The possible user cards then only serve to identify an individual counter related to a particular card or person. The agent in the vehicle can keep track of the consumption corresponding to said counter, and pass this information at appropriate moments to the rest of the traffic information system in the outside world. If one appreciates the possibility of recording counter values in user cards as well, for example because users then can read out the counter values at any desired moment, then the agents in vehicles simply have to ensure that a counter value, after modification, will be written back to the connected user card as well.

Manipulation with the counter value on a user card does not make sense if that counter value is only used informatively (i.e. only for the satisfaction of the user) and is not of decisive importance for correctly maintaining the correct counter value by the traffic information system. If the counter values on the user cards are indeed essential for the traffic information system, then they must be secured. This can be achieved, for example, with the help of cryptographic techniques and additional measures, but instead possibly also by relying (or partly relying) on the fraud resistance of the user card, which in this latter case probably will be a chipcard (and not a magnetic card). Only in this last-mentioned case of fraud-resistant chipcards (i.e. fraud-resistant from the point of view of the authority) with essential counter values, there is, during the use of the vehicle, besides the fixed agent also a second, loose agent in the vehicle.

But if the user card does include an agent anyway, then this agent could obviously also be used just as easily to take all agent tasks upon itself, so that the fixed agent in the vehicle can then be omitted. Now observe that the latter is not always possible. Only if the fixed agent had been fraud-resistantly attached to the vehicle in order to be able to also perform the vehicle identification and/or vehicle classification task in a very fraud-resistant manner, these two last-mentioned tasks cannot be taken over by the loose agent.

In short, we have demonstrated that usually one agent per vehicle can suffice. There also exist, as sketched above, real situations in which several agents are used per vehicle. Suppose one is inclined to use separate agents 1) for the vehicle identification and/or vehicle classification tasks, 2) for the function of consumption pass with counter, and 3) for the function of identification aid, the remaining agent tasks then being relegated, for example, to one of the used agents, which then thus becomes the 'general agent'. Then actually three agents would thus be necessary: one general agent and two specialized agents. But for the function of identification aid, an agent is not always really needed, as has already been suggested in Chapter 4. (For example, identification does not necessarily require the use of an agent if identification occurs by having a digital signature put.) Moreover, one can – and also generally will – combine the functions of identification aid and of consumption pass in one user card. In short, in the sketched situation two agents can, in general, easily suffice.

Note that for the vehicle identification and/or vehicle classification task an agent is necessary only if the fraud-resistant identification or classification of a vehicle is of importance for the correct functioning of the traffic information system. This is, for example, the case when the classification of a vehicle plays a role in the height of the tariff in case of traffic pricing. Finally, we point out once more that the use of a loose agent is an attractive option from the point of view of privacy protection (see also the previous section).

In summary, our argument boils down to the following. *One agent* can suffice. In any case, one fixed agent can suffice. But also one loose agent [can suffice], if very fraud-resistant vehicle identification or classification is not required for the correct functioning of the traffic information system. When using a loose agent, *two agents* are needed if very fraud-resistant vehicle identification and/or classification is/are also required.

Although there really can be a question of several agents (for example, because the tasks to be performed yet are distributed over a fixed and a loose agent/processor), we generally assumed and will assume, in simplification of the text, that this is not the case. Thus, we assume in this text (i.e. this elucidation of our invention) without loss of generality (i.e. solely for convenience) usually that at most one agent is involved – and sometimes that at most two agents are involved – per vehicle, and that the supervision and verification are performed by this single agent (or these two agents respectively). Although that is not necessary at all, we assume, in the case that several agents are used (anyway), that there is a question of one general agent and a number of specialized – relief – agents.

16.15 The use of agents as an attractive option

As has already been remarked more than once, the use of agents seems an attractive option for performing verifications and charging all kinds of traffic fees. It seems attractive to use an agent not only for keeping record of the due traffic fees and/or the consumed rights per person and/or per vehicle, but also for other tasks, such as, for example, the transmission of semi-identifications upon request (or almost continuously). The use of semi-identifications offers the advantage that the manager of the infrastructure can collect in a direct, but still privacy-friendly way all kinds of useful traffic information, such as, for example, information on traffic flows, traffic delays, utilization degree of roads, etc. In Chapter 18, we will come back to a number of tasks that an agent can perform.

17 Preparation for 'growth' of the system

By always appending to each message a protocol number (and possibly included in this number, or separately, a payment method number) and/or a message type number, one can, within one and the same system, allow differ-

ent systems or subsystems (such as, for example, versions) at the same time, and thus also support several levy structures and/or payment methods at the same time. In this way, one can start with a simple version of the system and then apply step by step extensions and refinements.

For example, one can choose to support in the beginning only one fairly simple protocol with a certain protocol number (e.g. number 1). Suppose that one does one thing and another as follows. Every vehicle is furnished with: 1) a transmitter and a receiver, 2) a fraud-resistant component that can act as agent, 3) a vehicle-related processor, i.e. a component for, among other things, checking messages from the agent and/or encrypting said messages for the sake of privacy protection, and 4) a central connection point to connect the just mentioned and possible future components to each other. One chooses one permanent hunter that also acts as the only intermediary. Each vehicle-related processor thus transmits, in case of this protocol, all messages from the agent destined for the final recipients, though after having them packed in a secret message to the hunter/intermediary, so that final recipients can only read the messages from the agent with the aid of that one hunter/intermediary.

With this first protocol the only task that the agent in each vehicle performs, is reacting to requests for identification. Upon each authorized request the agent identifies itself (and thus to a certain extent the vehicle) by signing such a request after addition of the time and an identification number, say its own identification number (or possibly the registration number of the vehicle for which the agent has been issued). This thus signed request is handed to the vehicle-related processor, which then enciphers it to a secret message for the hunter and which sends this secret message to the hunter via the transmitter of the vehicle. We assume that in first instance only open tolling is introduced. At all tolling points in question, the authorized hunter will query every passing vehicle, i.e. every passing agent, for identification. The hunter will strip every received response of the packing added for secrecy and then send the stripped message on to the fee collector, who charges the toll to the holder of the agent (or of the vehicle registration number).

Note that we did not require in our example that the agent be attached to the vehicle in a fraud-resistant manner. Even without fraud-resistant attachment, one thing and another may well indeed be sufficiently fraud-resistant. After all, interchange of authentic agents does not seem attractive. As long as passing of a tolling point leads, for each vehicle, to the same amount of toll, interchange with agreement of the registered holders of the agents (or of the corresponding vehicles) does not seem to make sense. Exchange with a stolen specimen perhaps seems attractive at first sight, because the bill then will be addressed to someone else, namely the robbed person. However, tracking a stolen agent down is sufficiently easy (at least, if that agent is actually used to have someone else pay for the toll) to minimize the appeal of such attempts to fraud. Of course, fraud-resistantly attaching agents to vehicles from the beginning is, at least if one has the disposal of a sufficiently cheap technique for that, also an attractive option, because then one is also prepared for applications in which fraud-resistant coupling of agents with vehicles is indeed desired or required.

As of a certain moment, one may require that new vehicles be prepared for being able to continuously deliver to the agent data concerning the kilometer counter value. They have to deliver the required information to the agent in the form of, for example, kilometer counter values (in, for example, two decimals), counter increases or pulses from a sensor on the driving shaft. At a given moment one can then change, for new vehicles, to the use of a second protocol (say, with procotol number 2), in which continuous pricing based on all traveled kilometers can also be used for the traffic pricing. Existing vehicles can also join after assembly of a sensor on the driving shaft. The connection of the sensor to the rest of the system is easy to implement, since we have arranged from the

beginning, by the installation of a suitable connection point, that the system is ready for connecting other vehicle equipment. Although the software in the agent may be already prepared from the beginning for this extension/adaptation, probably one thing and another will still need to be changed. For example, when pulses from a sensor on the driving shaft are used, the software may still require information about which distance covered by this vehicle corresponds to one pulse. (One might arrange that this information is also already present from the beginning.) Of course, the verifications described earlier (in Chapter 16) on the correctness of the kilometer counter values kept by the agent are now introduced as well.

The agent can also use the kept kilometer counter value – only at a later time or immediately in this second phase – for creating and transmitting semi-identifications based on the kilometer counter, for example for the benefit of collecting information on delays caused by traffic congestion. (With the first protocol, the agent could also already transmit, from the beginning, a fixed semi-identification, but not yet one of the kind in which the semi-identification is based on the kilometer counter and thus changes continually.) Immediately or at a later time again, one can also arrange, without any further modification of the hardware that is meanwhile present in vehicles, that the processor starts using software that makes the tariff of each kilometer dependent on the speed with which said kilometer was covered. (As has already been remarked before, said software could possibly also be supplied via the transmitters of the infrastructure, say alongside or above the road, and possibly also be put into operation automatically.) Also, one can add at some moment in time the possibility of using loose vehicle equipment (LVE), so that then the payer may be someone else than the holder or owner of the vehicle, and one can, if desired, introduce a system with tradable pollution rights. Etcetera, etcetera.

In completion of the above, we remark for the sake of clarity once again that, certainly as long as the tariffs of the traffic fee are the same for all kinds of participating vehicles (and the agent therefore does not have to supply reliable information on the vehicle classification), fraud-resistant connection of the agent to the vehicle can be omitted without presenting all too many difficulties. Fraud-resistant coupling, i.e. protection against exchanges of agents, is not necessary until a very high level of reliability of the classification and/or identification of vehicles by means of agents is required.

One can arrange that, for each combination of protocol and payment method, a separate protocol number is used. Instead of associating the payment method with a protocol number, one can also introduce a separate payment method number. With this number, it can be indicated in what manner one wishes to pay. For example, automatically via a bank account, per week or per month, with or without a credit facility, etc.

18 TIP systems

In the above, we have outlined various possibilities for obtaining a traffic information system with specific properties. To be able to obtain a traffic information system with the properties considered by us to be desirable, we have introduced a number of techniques, such as, for example, the creation of *semi-identification numbers* (either on the basis of counter values or not), the implementation of *speed checks* and the ascertainment of *traffic delays* with the aid of such semi-identification numbers, the implementation of *verifications* from a distance and/or in the vehicle on, among others, counter values, engine speed and fuel consumption, the fairly accurate computation of the *environmental pollution* caused, the use of *hunters* and/or *intermediaries* for the protection of privacy and the use of *agents* in vehicles for privacy protection and/or verifications.

In principle, a TIP system can use all the described techniques. But that is, as we have shown before, not necessary. For example, it is possible to implement a TIP system without agents and without user cards, thus without any fraud-resistant component in each vehicle. Also one may use agents in such a way that hunters and/or intermediaries are superfluous. Or one may, for example, decide not to use semi-identifications. In short, a TIP system will in general use only a part of the techniques described (and either characteristic or not). In general, one can already speak of a TIP system if at least one of the techniques (part-inventions) newly introduced by us – i.e. typical for TIP systems – is being used. In any case it is explicitly the intention that any use of one or several of the characteristic techniques *de jure et de facto* (i.e. by law and by facts) stands for an infringement on our invention.

18.1 A TIP system with agents

Precisely because there are so many mutually different possibilities to implement a TIP system, it seems wise to highlight, by way of illustration, one attractive option and to describe it as a coherent entity. We do this for the case of road traffic, choosing an approach with agents in the vehicles, since such an approach has a number of important advantages and does not seem to have serious disadvantages.

A clear advantage is that, with agents, much more information can be collected and verified without the costs sky-rocketing. After all, it is an easy job for an agent in the vehicle to *continuously* exercise close supervision, while the emphasis in case of the approach without agents is yet slightly more (or more clearly) on intercepting *random samples* of transmitted information for the benefit of verifications. In the approach without agents, information can indeed, in principle, be collected and verified almost equally intensively as in the approach with agents, but then only if the traffic network is swamped with transmitters, receivers and computers to make it possible to be in continuous contact with all vehicles and to process the enormous flood of information transmitted by the vehicles. Think especially of the much greater need for computing power, which then is required for the manifold use of hunters and intermediaries for the benefit of the desired privacy protection. In short, when using agents, intensive verification is possible with a much cheaper infrastructure, because then much less transmitters, receivers and especially also computers are needed than with the other approach.

From a slightly different point of view, one comes to the hereto-allied advantage that less communication is needed between the vehicles and the outside world than in the approach with all verifications from a distance. There will thus be a much smaller chance that the communication with many vehicles at the same time will lead to problems. It may be clear that the approach using agents indeed requires considerably less bandwidth for the communication between the vehicles and the outside world than the approach without agents. After all, each agent processes the data locally and may summarize the information and/or selectively transmit it, so that the communication with the outside world requires only a fraction of the bandwidth that would be required otherwise. (The bandwidth that otherwise would be required for the communication with the outside world is equal to the bandwidth required for the communication between the agent and the other equipment in the vehicle, such as sensors and measuring instruments.)

The only disadvantage of the approach with agents compared to the approach with only remote verifications is that a fraud-resistant component is required for each agent. This component will in general contain a chip with a processor and accompanying memory of which (a part of) the contents cannot be modified or even only read without authorization. However, this disadvantage does not carry much weight. Not only because such a compo-

nent does not have to cost much, but also because it seems unavoidable that, due to the need for sufficiently fraud-resistant vehicle identification and/or vehicle classification, a fraud-resistant component with a chip must be attached to the vehicle anyway.

Therefore it is fairly obvious to opt for an approach with agents, and possibly to use each agent also for the fraud-resistant holding and supplying of reliable vehicle information. By vehicle information we mean: 1) data that – more or less – identify a vehicle, such as chassis number, engine number, vehicle registration number, etc., 2) data that characterize a vehicle, such as, for example, brand, model, year of manufacture, gearbox type and/or engine type, and 3) other information on the vehicle, such as, for example, permitted kind of fuel or fuels, weight, color and/or information on the legitimate holder or owner, such as, for example, his or her social security number or his or her name and address.

When once the choice for an approach with agents has been made, it must then still be decided which tasks the agents will perform. An agent can, if desired, perform a plurality of tasks, of which we here will enumerate a number in the context of road traffic.

1. *Collecting* and/or *keeping record* of all kinds of information, considered to be relevant, on the *use* of the vehicle, on the basis of information supplied by equipment in the vehicle (particularly, sensors and/or measuring instruments).
   Think, for example, of information such as speed, engine speed, kilometer counter value, fuel consumption, fuel counter value, temperature and the like. Note that these data are, in general, fairly dynamic, i.e. that now and then they will be subject to fairly frequent changes.
2. *Verifying* (directly or indirectly) whether said supplied information is sufficiently reliable and/or correct.
   For this purpose, use is often made of reliable information supplied from the outside world. Think, for example, of – direct – verification of the speedometer, kilometer counter and outside temperature meter and, for example, of – indirect – verification of the revolution counter and fuel consumption meter.
3. *Reporting* at appropriate moments to an – authorized – verifying authority in the outside world the findings of the checking activities.
   Think, for example, of the reporting on possible irregularities or of – apparently – flawless operation.
4. On the basis of available information *computing* and/or keeping record *of derived information.*
   Think for derived information, for example, of a fairly accurate computation of the fuel consumption and/or of the pollution caused at a certain moment, in both cases on the basis of other data, such as, for example, brand, model, year of manufacture, gearbox type, engine type, speed, engine speed, acceleration, fuel consumption[53], outside temperature, engine temperature and the like. Think also of a fairly accurate computation of the noise production. For the computation of derived information from other data, the agent of course needs to have the disposal of a method of computation, for example in the form of a formula or of one or more tables.

---

[53] Of course, this item belongs only to this enumeration in case of the example of the computation of environmental pollution caused.

- 8 SEP 2003

The derived fuel consumption can, in particular, be used to – indirectly – verify the reliability of the fuel consumption as reported by the vehicle. The derived pollution can be used for maintaining a counter for the total environmental pollution caused.

5. Occasionally and at appropriate moments, *supplying* specific – reliable – information on the *use* of the vehicle to a specific authorized authority in the outside world.
   This supply may, for example, be performed for the sake of imposing and collecting traffic fees and/or traffic fines. Think, for example, of supplying specific counter values together with identifying data of the corresponding vehicle (or its user, payer, holder or owner) for the benefit of imposing and collecting a continuous fee, and of supplying data concerning traffic offenses possibly established by the agent. Certain fines may have been already integrated in the tariffs of a traffic fee.

6. Collecting and occasionally supplying specific information to a specific – authorized – authority in the outside world for the benefit of acquiring *statistical real-life data.*
   Think, for example, of the supply (selective or not) of data on the fuel consumption, reported by the vehicle, in various circumstances (characterized, for example, by speed, acceleration, engine speed, outside temperature, engine temperature and the like) with accompanying notification of the vehicle type, so that the authority in question can obtain a good impression of the fuel consumption of vehicles of that type (i.e. brand, model, year of manufacture, gearbox type, engine type and the like) in practice.

   Such – statistical – real-life data may be used, for example, to find algorithms for the benefit of determining derived information.

7. The fraud-resistant storage and disclosure of vehicle information.
   The disclosure of vehicle information should only occur, certainly if this information concerns holder/owner or vehicle identifying information, under specific, clearly described conditions and/or in specific, clearly described circumstances, and even then preferably only to one or more specific authorities in the outside world that are deemed relevant. Note also that vehicle information is in general rather static, i.e. it will not, or rather infrequently, be subject to changes.

8. (Constructing and) forwarding of a *semi-identification number* upon request of an authorized authority.
   This number may be derived, for example, from the kilometer counter value and may be used by the authority in question, for example for determining traffic delays resulting from traffic congestion, verifying whether the average speed on a specific route has been kept below the speed limit, studying traffic flows, performing traffic census, etc.

9. *Verifying* the authenticity of received messages concerning the infrastructure and *forwarding messages* to other equipment in the vehicle.
   Thing, for example, of forwarding official messages about speed limits, traffic delays, the outside temperature, the position, the speed, and the like.

10. Only if a card (or user card) can or must be used during the use of the vehicle, taking care of the *communication with* the offered user card *or*, if the agent itself is located on said card, itself *performing* (or also performing) *the function of user card* (consumption pass).

-8 SEP 2003

Said communication may relate to, among other things, the mutual verification on authenticity, the exchange (in so far as applicable and desired) of identifying data and/or the sufficiently frequent updating of the correct counter value on the card.

Note that the user card may contain an anonymous or a personal counter value, and that the updating of a counter value thus may concern, for example, the repetitive decreasing of the counter value on an anonymous or anonymously sold user card, or, for example, the repetitive increasing of a personal counter value on an identifiable payer or user card.

11. After receipt of an appropriate request signed by the legitimate holder or owner (or after receipt of a password previously supplied by the legitimate owner/holder) taking care of *frequent transmission of identifying data*. Hereby it often becomes relatively simple to track the vehicle concerned quickly, for example after theft.

12. Acting as reliable taximeter, tachograph and/or black box, and the like.
The adjective 'reliable' here concerns (besides the fraud resistance of the equipment in question itself) particularly the verification of the correctness of the information (or a part of the information) supplied to it (i.e. its input).

Of course, an agent does not necessarily have to perform all (whether or not mentioned) tasks, and one may choose for a – possibly small – subset. The above does really illustrate once more the broad applicability of the TIP system, i.e. that the TIP system is also suited for use as a multifunctional (either integrated or not) traffic information system.

An agent is by definition a fraud-resistant component. Here we emphasize, abundantly, that for certain tasks it is also necessary that the agent is *fraud-resistantly coupled* (and thus remains coupled) to the correct, corresponding vehicle.

18.2 Components being part of the TIP system

In the case of a TIP system, the traffic information system consists of, among other things, a large number of mutually communicating computers, of which, when using agents, a substantial number (namely, each agent) will be located (possibly only during use) in the vehicles involved and therefore will be mobile. Thus, in our judgement, an agent forms part of the traffic information system. For possible user cards (say, magnetic cards or chip-cards) that users may have with them and that are not covered by the notion of agent, the choice is somewhat less clear. If these serve mainly for retaining and/or maintaining TIP system related personal or non-personal usage rights, pollution rights and/or other counter values, we consider these to be parts of the total system. All other vehicle equipment can be considered not to be part of the TIP system. Thus, it is not necessary to consider vehicle-resident components, such as, for example, sensors and/or measuring instruments, to be parts that belong to the TIP system, not even if these components supply information that is useful or even necessary for the operation of the TIP system in question.

18.3 TIP-agents

Because of the many and diverse tasks that the TIP system can perform, it is very well imaginable that all applications are not covered by one and the same authority. In such a case one of the authorities involved, or a separate authority that is independent of the authorities involved with the applications, may be responsible for the operation of the TIP system. If so, then an agent can be seen primarily as a representative of the authority respon-

- 8 SEP 2003

sible for the TIP system, and only secondarily as representative of the authority or authorities involved with the applications, who apparently have sufficient confidence in the agents (and the rest of the TIP system) to entrust (or dare to entrust) them with certain tasks.

18.4 TIP systems for other traffic

The enumeration of tasks that an agent can, among other things, perform, was given in the context of road traffic. It is not so difficult to make a similar enumeration for a number of other forms of traffic. We do want to emphasize here that the outcome of weighing an approach with agents against one without agents can differ for each form of traffic. For example, this is true for the case of air traffic, where tracing of commercial aircraft in general is not considered to be a privacy threat. In case of the earlier sketched example of reducing noise nuisance, one thus can do also very well without agents.

One then requires, for example, that aircraft within a certain distance from a certain airport must – almost – continuously transmit information on their position and on the noise that they produce. The correctness of the given position can be verified regularly (by means of radio-bearings and/or radar installations or the like). The noise production can be spot-checked, with a reasonable degree of accuracy, on correctness or, better formulated, on reliability, by performing – particularly ground-based – sound-measurements [alternative translation: sound-ranging] on various locations in the vicinity of approach and fly-out routes. By collecting sufficient knowledge about the propagation of sounds and sound-levels (in both cases dependent on a number of circumstances, such as, for example, wind direction), one can derive by computation from the noise level information supplied from the airplane how much noise approximately should have been observed at the measuring point and thus verify whether this derived value does not deviate too much from the value actually measured.

It is clear that one can verify the correct following of the prescribed approach route anyway. Besides that, one can then check whether the airplane in question has produced too much noise or not. By possibly describing the flying routes as fixed 'allowed noise contours', one may reduce noise nuisance in an efficient and flexible way. Less noisy aircraft then will have some more freedom of movement within the fixed contours than more noisy ones. And will also less easily exceed the imposed noise limits if, for example, during landing it appears necessary to intermediately open the engine throttle. Fines, if any, can then of course be made dependent on the seriousness (duration and amount) of the noise limit violation. Airline companies will then have an interest in avoiding fines and will stimulate their pilots (for example by means of a bonus and/or penalty system) to stay within the noise contours. With more noisy machines in particular, the desired approach or fly-out route then will be followed more accurately. That is not only favorable for those that have to undergo the noise nuisance, but also for an airport. After all, an airport will then less quickly be forced to take 'black/white decisions', i.e. will then have the advantage that it does not immediately have to completely exclude a somewhat noisier machine (and particularly 'borderline cases').

CLAIMS:

1. Method for the collection of traffic information by or on behalf of an authority

a) in which during the traffic participation of a vehicle involved:

1) vehicle equipment supplies traffic information to one or more processors present in said vehicle

2) said processor or processors process said information and keep record of certain traffic information on the use of said vehicle

3) said processor or processors transmit certain traffic information to outside said vehicle by means of a transmitter present in said vehicle

b) that is characterized by the combination of properties that:

1) the traffic information collected by or on behalf of the authority includes values of counters that are associated with individual vehicles and/or persons and that during traffic participation are kept up-to-date by said processors in the vehicles involved,

2) during the traffic participation of a vehicle involved said processor or processors transmit certain traffic information continually, and at least at a prescribed rate, to outside said vehicle by means of a transmitter with a prescribed range

in order to make said information available to outside said vehicle in such a way that the authority has the ability to gain access to said transmitted information at any desired moment by placing a receiver within the range of the transmitter of said vehicle

3) remote spot-checks by surprise are used to verify the reliability of the values of said counters

4) such a spot-check by surprise from outside a vehicle being checked comprises

intercepting one or more samples of the traffic information that is continually transmitted from said vehicle during its traffic participation as described in the first half of clause b.2, by means of a receiver that is placed within the range of the transmitter of said vehicle as described in the second half of clause b.2, and

comparing said intercepted sample or samples of the traffic information transmitted from said vehicle with traffic information concerning said vehicle that has been independently determined at a distance from and outside said vehicle.

2. Method according to claim 1 in which the messages with traffic information made available to outside a vehicle involved as described in clause b.2 of claim 1 include: 1) the position of said vehicle, or 2) all or part of the value of a counter as described in clause b.1 of claim 1, or 3) the increase or decrease of said counter, or 4) a speed indication.

3. Method according to claim 1 or claim 2 in which the traffic information that is described at the end of clause b.4 of claim 1 and with which intercepted samples are compared, is determined by independent measurement.

4. Method according to a preceding claim in which during the traffic participation of a vehicle involved the processor or processors in said vehicle, as described in claim 1, keep one or more counters, as described in clause b.1 of claim 1, up-to-date based on information on distances traveled by said vehicle that is supplied to said processor or processors by a sensor or measuring instrument present in said vehicle.

5. Method according to a preceding claim in which said remote spot-checks by surprise are used to verify whether said counters are continually incremented, or decremented, correctly.

6. Method according to a preceding claim in which said counters are used for continuous pricing.

7. Method according to one of the preceding claims 1-5 in which said counters are used for traffic pricing.

8. Method according to claim 6 or claim 7 in which the tariff can vary for each distance unit traveled.

9. Method according to claim 8 in which the tariff for each distance unit traveled can be made dependent on the speed with which said distance unit has been traveled.

10. Method according to claim 8 or claim 9 in which the tariff for each distance unit traveled can be made dependent on the location where and on the date and time when said distance unit has been traveled.

11. Method according to one of the preceding claims 2-10 in which the messages with traffic information made available to outside a vehicle involved as described in clause b.2 of claim 1 include the values of a counter as described in clause b.1 of claim 1 and in which said counter is an odometer or a fuel consumption counter or a cumulative revolution counter or a traffic fee counter or a noise production counter or an environmental pollution counter.

12. Method according to a preceding claim in which a spot-check as described in clause b.4 of claim 1 comprises the interception of a sample of traffic information, as described in clause b.4 of claim 1, from the vehicle being checked both when entering and when leaving an inspection trap that can only be entered via one of its entrances and only be left via one of its exits and for which the length of each trajectory from an entrance to an exit is known with sufficient accuracy.

13. Method according to a preceding claim in which, for the verification of the reliability of the values of a counter, a spot-check as described in clause b.4 of claim 1 is carried out with the help of a difference quotient or derivative.

14. Method according to one of the preceding claims 2-13 in which:

1) remote spot-checks by surprise are used to verify the monotony of said counters

2) such a spot-check comprises intercepting a value of said counter transmitted from a vehicle involved as described in claim 2 and comparing this intercepted value with a value of the same counter that has been intercepted previously.

15. Method according to a preceding claim in which the further processing of the traffic information outside the vehicles involved does not require all traffic information transmitted from said vehicles to be retrieved by or on behalf of the authority outside said vehicle.

16. Method according to one of the preceding claims 1-14 in which only part of the enormous flood of traffic information being continually transmitted from the vehicles involved is collected and processed, since it is not made possible for the authority to be in continuous contact with vehicles during their traffic participation.

17. Method according to a preceding claim in which the traffic information being transmitted continually from a vehicle involved, as described in clause b.2 of claim 1, is transmitted by means of infrared light.

18. Method according to a preceding claim in which said remote spot-checks are performed from mobile checkpoints.

19. Method according to a preceding claim in which the processors described in claim 1 include a processor on behalf of the authority and in which said processor can only obtain access to the transmitter in said vehicle via a processor on behalf of the user, owner or holder of said vehicle in order to allow supervision on the messages transmitted by the processor on behalf of the authority.

20. Method according to a preceding claim in which tracing of individual, uniquely identifiable persons and/or vehicles is prevented by having all or part of each message with traffic information made available as described in clause b.2 of claim 1 -at least- doubly enciphered, once to make all or part only readable for the authority and once more thereafter to make the result only readable by a privacy protecting organization that is independent of the authority, in order to make that reading of the doubly-encrypted part or parts requires the cooperation of -at least- two independent organizations, viz. the authority and said privacy protecting organization.

21. Method according to a preceding claim in which during the traffic participation of a vehicle involved a receiver is used in said vehicle to limit the continual transmission described in clause b.2 of claim 1 to periods after authorized requests or orders.