eSecurity Working Group

Vulnerabilities in Electronics and Communications in Road Transport: Discussion and Recommendations

Title:	Vulnerabilities in Electronics and Communications in Road Transport: Discussion and Recommendations
Project:	eSecurity Working Group
Editor:	Trialog
Date:	21 June 2010
Version:	v1.0
File:	eSecurity_VulnerabilitiesInRoadTransport_v1.0.doc

Document History

Version	Status	Date
0.1	Introduction + Use Case + Legal Part, BASt	02.12.2008
0.2	Integration of OEM contribution Integration of section from previous draft report further to 7th plenary meeting (6 Feb, 2009), Antonio Kung	17.06.2009
0.3	Restructuring the 2 parts : Independent Vehicle-based Electronics Interactive Systems	18.06.2009
0.4, 0.5	Contributions on use cases and measures related to the privacy of today location oriented services Some comments on cooperative systems sections	01.09.2009
0.6	Restructuring part 2	01.10.2009
0.7	New sections: 3.2.1.2 Unauthorised Access to Data in the Road Charging Service 3.2.2.2 Unauthorised Access to Data in the Road Charging Service 3.2.1.3 Unauthorised Access to Data in the Pay-as-you-drive Service 3.2.2.3 Unauthorised Access to Data in the Pay-as-you-drive Service 3.3.2 Discussion Legal Consequences Future Cooperative Systems 3.3 Security and Privacy of Future Cooperative Systems	06.11.2009
0.8	Small text corrections: 3.2.1.2, 3.2.2.2, 3.2.1.3, 3.2.2.3, 3.3 New sections: 3.2.1.1 Unauthorised Access to Data in the eCall Service 3.2.2.1 Unauthorised Access to Location in the eCall Service	01.12.2009
0.9	English corrections: grammar, spelling, etc. 2: Part I Deleted: 3.3.2.1 Legal constraints 3.3.2.2 Warranty aspects 3.3.2.3 Liability aspects 3.3.2.4 Privacy aspects	09.12.2009
0.91	Adding organisation measures in part 2 Adding conclusions in part 1 and part 2 Elimination of state of the art section (will be transferred in a working document) List of members	30.12.2009
0.92	More explanative title Organisation and hyperlinks for references	05.01.2010
0.93	Review before submission to working group	06.01.2010
0.94.6	Move all motivation and contents to beginning Introduction section Roll back of Part 1 to version 8, with updates Updates to legal sections in Part 1 (2.2) & Part 2 (3.3) New version of section 3.2.1 Road Charging Addition of Recommendations section at end	15.04.2010
0.95	Accept all modifications of v0.94.6_JH Treat comments v0.94.6_JH according to discussion 20 April meeting Revised recommendations Introduction of Contents of Part 1 moved to Part 1 Introduction added for Part 2 Small corrections of spelling and grammar	30.04.2010
0.96	Minor corrections of T. Gasser and J. Scholten	10.06.2010
0.99	Version for last review	10.06.2010
1.0	Final version Definition of privacy updated in section 3.3.2.1	21.06.2010

Table of Contents

1 Introduction

Intelligent Transport Systems (ITS) bring the promise of more safety, comfort, security, environment preservation and energy consumption reduction. However, the resulting increase in electronics and communications is raising security and privacy issues that could jeopardise deployment. The eSecurity Working Group was set up within the eSafety Forum as a discussion platform involving all stakeholders with two objectives: to discuss vulnerability aspects of electronics and communications in road transport while taking into account existing practice and emerging Research and Technology Development (RTD) initiatives, and to agree on recommendations to improve or eliminate the vulnerabilities.

This report is divided into two parts:

- Part 1: Independent Vehicle-based Electronics deals with in-vehicle products and systems, such as electronic components, pre-fitted on-board systems, and after-market additional vehicle electronics (known as “nomadic devices”). This report refers to those products and systems as *independent vehicle-based systems*.
- Part 2: Interactive Systems deals with overall applications involving vehicles communicating with external systems, for services such as road charging and Intelligent Transport Systems. This report refers to those systems as *interactive systems*.

The separation of the topics in these two parts is necessary because the scope and level of understanding of security issues are different. Independent vehicle-based electronics have been deployed for many years by the automotive industry. Many electronic systems are integrated in vehicles today, and a wealth of experience is available. Vulnerabilities are already known and addressed. On the other hand, interactive systems are located in an evolving and changing environment. New technologies such as car-to-car communication are anticipated. Not much experience is available on vulnerabilities or how to address them.

1.1 Motivation for Part 1: Independent Vehicle-based Electronics

Since electronic systems have found their way into most areas of modern life, awareness of possible misuse and manipulation has immensely increased. This awareness is – due to severe problems in the field of personal computing – however still rather limited to this field. But even if in comparison this matter must presently be considered of minor importance, misuse and manipulation already take place in the field of traffic and transport as well.

Vehicles of the 70’s and early 80’s did not include many electronic systems, so the manipulation of electronics was no issue. Some possibilities for manipulation – quite similar to those we are facing today – already existed nonetheless. This was, however, usually achieved by means of physical manipulation and thus required different skills. The increasing number of vehicle electronics potentially enlarges the number of possibilities for electronic manipulation. Many of these components, however, are of no interest as far as manipulation is concerned. Apart from this, the increase in security – as e.g. apparent with vehicle locking systems – has considerably increased since the originally mechanical components have been replaced by electronics. However, complete security is impossible to achieve. Furthermore, as long as manipulation is not effectively barred by security measures (which might not be possible to full extent), electronic manipulations are hardly retraceable.

It must be noted that misuse and manipulation are problems arising within the sphere of users. In this report, the targets include products such as vehicle components, pre-fitted on board systems, and after market vehicle electronics (“nomadic devices”). In most cases, these products are either deliberately applied beyond their intended use or beyond system limitations (misuse), or they are intentionally modified in order to achieve some kind of benefit which is in some cases illegal (manipulation).

1.2 Motivation for Part 2: Interactive Systems

The part on interactive systems addresses two problems which have raised concerns in the ITS community:

- The privacy of location based applications. Such applications utilise vehicle location information, using technologies such as satellite navigation systems. Examples of such services are road charging and pay-as-you-drive insurance. The implementation of such services involves the collecting, transmitting and processing of information which could be related to individuals, therefore raising privacy issues.

- The security and privacy of future co-operative systems applications. Such applications rely on vehicular communications (VC) and inter-vehicular communications (IVC) capability that are foreseen in the future. Examples of such applications include extended hazard warning in safety critical situations, applications to achieve high throughput in merging areas, extended blind spot applications, safe overtaking, and safe lane change assistance.

1.3 Report Content

Contents of Part 1: Independent Vehicle-based Electronics:

- In section 2.1, some relevant issues for security are described in the form of use cases which are meant to improve the understanding of the scope of the problems.
- In section 2.2, legal regulations that are in existence and applicable to electronic misuse and manipulation are described.
- In section 2.3, the availability and effectiveness of preventive measures presently taken by manufacturers are reviewed.

Contents of Part 2: Interactive Systems:

- Section 3.1 presents the privacy vulnerabilities of location-based applications.
- Section 3.2 presents the legal context of interactive systems.
- Section 3.3 discusses the security and privacy of future cooperative systems.

1.4 Working Group Participants

1.4.1 Chairmen

Last Name	First Name	Organisation
Kung	Antonio	Trialog
Ruland	Christoph	University of Siegen

1.4.2 Working Group Participants

Last Name	First Name	Organisation
Reinhardt	Wolfgang	ACEA
Polli	Roberto	Altea
Seeck	Andre	BASt
Gasser	Tom	BASt
Vierkötter	Marcel	BASt
Scholten	Joachim	BMW
Offermann	Tobias	Bosch
Eymann	Thomas	Bosch
Younès-Fellous	Vanessa	CNIL
Carvais	Johanna	CNIL
Cosenza	Stefano	CRF Fiat
Held	Albert	Daimler
Müter	Michael	Daimler
Franz	Walter	Daimler
Leinmueller	Tim	Denso
Mäurer	Hans-Jürgen	Dekra
Papadimitratos	Panos	EPFL
Pellischek	Gloria	ERPC GmbH
Bridgeman	Gary	ERTICO - ITS Europe

Carrotta	Alessandro	ERTICO - ITS Europe
Konstantinopoulou	Lina	ERTICO - ITS Europe
Buchta	Anna	European Commission
Surmont	Charles	European Commission
Davila	Emilio	European Commission
Höfs	Wolfgang	European Commission
Okagoglou	Gzim	European Commission
Gerlach	Matthias	Fraunhofer Fokus
Dölle	Lukas	Informatik HU BERLIN
Freytag	Christoph	Informatik HU BERLIN
Kost	Martin	Informatik HU BERLIN
Chatfield	John	InnovITS Ltd
Ernst	Thierry	Inria
Ngoh	Lek Heng	Institute for Infocomm Research (I2R) Singapore
Osório	Luís	ISEL
Deckers	Sebastian	ITM - Öffentlich-rechtliche Abteilung (Abt. II)
Troncoso	Carmela	Katholieke Universiteit Leuven / COSIC
de Cock	Danny	Katholieke Universiteit Leuven / COSIC
Stevens	David	Katholieke Universiteit Leuven / ICRI
Dumortier	Jos	Katholieke Universiteit Leuven / ICRI
Yiangoullis	Yiango	Katholieke Universiteit Leuven / ICRI
Geuens	Christophe	Katholieke Universiteit Leuven / ICRI
Trenor	Tomas	LISITT - Instituto de Robótica
Vila	Marta	LISITT - Instituto de Robótica
Perez Losa	Pedro Alfonso	LISITT - Instituto de Robótica
Vila	Marta	LISITT - Instituto de Robótica
Sansone	Fulvio	Mediamuse
Daulaud	Claude	Ministère de l'industrie
van Rongen	A.K.	Mobi-Spot
Godart	Julie	NAVTEQ
Motte	Stefaan	NXP
Karppinen	Lauri	Office of data protection Ombudsman
Lonc	Brigitte	Renault
Foersterling	Frank	Siemens VDO
Janusson	Ulrik	Sweco VBB
Venema	Nol	Technolution
Rebuffi	Luigi	Thales
Susta	Antonin	The Office for Personal Data Protection
Kung	Antonio	Trialog
Raither	Barbara	Trialog
Bartsch	Markus	TÜV Informationstechnik GmbH
Holle	Jan	University of Siegen
Groll	André	University of Siegen
Ruland	Christoph	University of Siegen
Zhendong	Ma	Ulm University
Kargl	Frank	Ulm University
Spell	Sabine	Volkswagen
All	Pontus	Volvo
Thorngren	Jonas	Volvo
Gaillet	Jean-François	Ygomi LLC

1.4.3 Acknowledgements

We would like to thank the following people for their editorial contributions:

Last Name	First Name	Organisation
Gasser	Tom	BASt
Vierkötter	Marcel	BASt
Scholten	Joachim	BMW
Konstantinopoulou	Lina	ERTICO - ITS Europe
Troncoso	Carmela	Katholieke Universiteit Leuven / COSIC
Daulaud	Claude	Ministère de l'industrie
Motte	Stefaan	NXP
Venema	Nol	Technolution
Kung	Antonio	Trialog
Raither	Barbara	Trialog
Ruland	Christoph	University of Siegen
Holle	Jan	University of Siegen
Kargl	Frank	Ulm University
Spell	Sabine	Volkswagen
Ohst	Daniel	Toll Collect

We would also like to express our thanks for the participation of members of the Article 29 Working Group Party[1].

[1] The Article 29 Data Protection Working Group Party is an independent European advisory body on data protection and privacy [12]. Its tasks are described in [37][38].

2 Part 1: Independent Vehicle-based Electronics

The amount of electronics in traffic systems is increasing fast. Many are already integrated in today's vehicles. Consequently some possibilities for misuse and manipulation of electronics are known. Part 1 of this report deals with the cases that are known today. In the first section, some issues, described as use cases, of relevance for security are presented. These use cases are meant to improve the readers' understanding of the scope of the problems. Then legal regulations that are currently in force are pointed out, according to German legislation. Finally, possible gaps are identified that can be handled by technical security measures, at least as long as legal provisions prove to be non-effective and the danger is substantial.

2.1 Vulnerabilities Use Cases

This section describes a number of presently known cases of misuse and manipulation of electronic vehicle systems. They are meant to clarify the scope of Part 1.

2.1.1 Unauthorised Enhancement of Engine Power

The unauthorised modification of a vehicle's characteristics by reprogramming the engine's electronic control unit (ECU) or the integration of additional electronic components (known as "chip tuning") has a negative impact on not only the engine itself. In most cases, the safety relevant components in the vehicle will not match the new unauthorised adjusted power characteristic. This can cause incalculable consequences for the vehicle occupants and the surrounding traffic. In addition to the safety aspects, it is extremely complicated to retrace the modification of the engine after removing the manipulated software or hardware. In this case, the modification may also have an impact on the interest of vehicle manufacturers to maintain vehicles in its original condition. The reason lies in the OEM's obligation in terms of, for example, the warranty.

2.1.2 Unauthorised Mileage Adjustment

To increase the value of a vehicle, the mileage might be adjusted. In some Member States this is even offered as a special service by some garages. Usually this is done by some intelligent electronic equipment which is plugged into the vehicle and allows mileage adjustment. After this, the vehicle will often be sold without informing the buyer about the adjustment. This is an act of fraud against the new owner. Another aspect is that the new owner does not know how old the components in this vehicle are and is thus exposed to a safety risk. If it is not possible to retrace the unauthorised adjustment, then this might also be fraud against service garages, manufacturers and insurance companies. This is because insurance coverage and warranty on spare parts and vehicles is limited by a certain mileage.

2.1.3 Unauthorised Points of Interest in Digital Maps

Electronic maps in navigation systems offer several additional options. One of them is the display of interesting points (e.g. hotels, bars, restaurants) along the route. Depending on the Points of Interest (POI's) integrated, it is possible to warn of radar control units at the roadside. This is not only critical from a safety point of view, but also legally because the use of this information is prohibited by law in some Member States. Inconsistent to this, selling such maps is not prohibited. In addition, consumers are often unaware of such bans in certain Member States.

2.1.4 Unauthorised TV, DVD or Internet Access in Moving Vehicles

More and more navigation systems offer TV or DVD functions in the car. In addition, it will be possible to access the internet in the near future. Normally the integrated TV, DVD and internet functions are only available if the vehicle is not in motion or moving below walking speed (below 6 km/h). By pressing a combination of keys or the simple installation of some freely available electronic components in the CAN-Bus (Controller-area network bus: an in-vehicle communication system for electronic components), it is in some cases possible to avoid this limitation. This applies mainly to vehicles with older hardware and software. The modification of these electronics can cause incalculable consequences for the vehicle and the surrounding traffic. The underlying risk in this kind of manipulation is distraction of the driver which generates a risk for traffic safety. From a legal point of view this case is disputable too (see section 2.2.4). Such dangers to security are usually even greater with retrofit systems. Later integrated systems of third-party manufacturers or handheld nomadic

devices have no or little protection against the possibility to use the mentioned functions while driving. That means that manipulation, as mentioned before for integrated systems of OEMs, is not necessary in the first place.

2.1.5 Other Possibilities for Intentional Manipulation

Vehicles contain more and more electronics for comfort and safety applications. In the case of some comfort applications, there is a risk of unexpected manipulation. e.g. the electronically controlled convertible top. In the case of manipulation, it can be possible to open the top with a remote key, and this can even be achieved when driving up to speeds of 60 km per hour. Such hardware manipulation is available without permission by vehicle manufacturers. The manipulation of the convertible top is in some cases easily achieved by some electronic hardware in the CAN-Bus.

Other scenarios of intentional manipulations are imaginable, e.g. the possibility of adjusting a shorter distance to vehicles in front with an Adaptive Cruise Control (ACC), or the deactivation of a hands-free detection of the steering wheel in case of a lane-keep assist.

These scenarios are also relevant for traffic safety and they touch the interest of the manufacturer, because warranty aspects can generally not be excluded.

2.2 Discussion on Legal Consequences

Misuse and manipulation are problems arising within the sphere of users. In most cases products (in this report: vehicle components, pre-fitted on-board systems, after market vehicle nomadic devices, etc.) are either deliberately applied beyond their intended use or beyond system limitations (misuse) or they are intentionally modified in order to achieve some kind of benefit which is usually legally disapproved (manipulation).

In legal terms and as far as product liability is concerned, manufacturers will generally not be considered liable, as misuse and manipulation are beyond their sphere of influence. Even so, manufacturers take precautions to avoid misuse and manipulation. Yet in spite of manufacturers' professional approach, the great number of often ingenious users with excellent knowledge on how to manipulate electronic systems should not to be underestimated (a lesson to be learned from the parallel situation with security dangers in personal computing). Furthermore, when designing a product, it will often prove impossible to anticipate or even overview all the possibilities for future misuse and manipulation. It must therefore be considered neither just nor equitable to hold a manufacturer liable if misuse or manipulation by the user has not been encouraged. The complete absence of legal consequences is, however, questionable in case a manufacturer incites misuse or manipulation, e.g. by providing necessary tools and information.

On the other hand, the legally permitted customisation of vehicles is a legitimate interest of the user. The following examples are therefore valid and only in so far of legal relevance, if a law is in place at all. This section will therefore focus on the legal consequences such manipulation has nowadays in certain fields and point out the limited possibilities and effects the law may have, exemplified by the legal situation in Germany.

2.2.1 Unauthorised Enhancement of Engine Power

Some vehicles are customised by their owners. Optical modifications, generally speaking, tend not to be as safety critical as they are visible from the outside, and dangers can be uncovered more easily (e.g. by the police or through periodical technical inspections). Greater dangers are involved in the case of an unlicensed enhancement of engine power. It is important to point out that possible concerns and consequences described here are absent in the case of a licensed enhancement of engine power. As chip tuning may lead to an increase in insurance premiums, taxes (as exhaust emissions may be affected), or not be licensable at all, there is a risk that this is done illegally, i.e. without any knowledge on the side of the insurer, or the registrations office (such modifications are registered, if authorised). Modifications will usually not have been approved by official technical experts either. Moreover, some possibilities for manipulation of electronics even allow for instant "deadening" so that manipulations cannot be uncovered by the police or during a general inspection.

In addition, as soon as electronics have been put back to the original condition, retraceability is barred as electronic modifications can hardly be retraced,, at least as long as no long-term data is stored. It must, however, be pointed out that data storage might cause concerns in terms of data privacy (and is therefore not a favourable alternative). Technical solutions that bar the possibility of manipulation in the first place have the advantage that customers will not feel uneasy about the extent of data

recorded, which they feel they might not be able to inspect. A technical solution furthermore has a greater effect on traffic safety as manipulations are made impossible in the first place.

The legal consequences of the unauthorised modification of an engine's power are manifold. First of all, the vehicle's operating license will usually expire. The licensing of a vehicle for Europe is generally taken out by means of type approval according to technical rules and regulations in international law. For Europe the ECE-Regulations (Economic Commission for Europe) are binding and their fulfilment is considered sufficient for road admission throughout Europe. It is this operating license that is no longer applicable to the illegally power-enhanced vehicle in question. For example, in Germany such unauthorised modifications lead to the expiry of the vehicle's operating license (Section 19 paragraph 2 of StVZO: the German Road Traffic Licensing Regulations [34]). Again, note that the legal consequences and concerns do not apply in the case of licensed engine power enhancement.

The following three aspects are subject to examination in the case of licensed modifications, as they might be negatively affected in case of power enhancement:

- Noise emissions of power-enhanced vehicles tend to change. As far as the admission to the road is concerned, whether the vehicle remains compliant with technical emissions requirements after an authorised modification would be subject to an expert report.
- Traffic safety may be affected since the brakes of a power-enhanced vehicle may no longer match the vehicle's power potential. This would likewise be subject to an expert report in the case of an authorised modification. It must, however, be pointed out that the brakes of automobiles nowadays more than meet technical requirements in terms of brake power, so that possible power enhancement will rarely be in conflict with this requirement. This can, however, be the case with small motorcycles, scooters, etc.
- The vehicle's exhaust emissions might be affected too. This again is subject to expert supervision in the case of authorised modifications.

Finally, a vehicle's operational hazard will rise due to the power enhancement. This has an effect on the road traffic liability risk which the vehicle brings about and must be insured. In case of an accident with an unlicensed increased-power vehicle, the insurance company would (e.g. in Germany) remain liable even though this no longer belongs to the insured risk. However, the insurance company then has the possibility to gain recourse from the contractual partner breaching contractual obligations to disclose such an enhancement in engine power. In case recourse for substantial damages cannot be reimbursed to the insurance company, the damage will naturally remain with the insurance company which will lead to an increase in insurance premiums.

2.2.2 Unauthorised Mileage Adjustment

As described in section 2.1.2, the unauthorised adjustment of mileage is usually fraud against the new owner of the vehicle. If the mileage is reduced, the vehicle can usually be sold at a higher price since the buyer believes the value to be higher than it would be with the true mileage. Such manipulation of mileage recorders is a problem that has been known for quite some time. However, there has been a substantial increase in number of fraudulent manipulations since this now can easily be achieved by electronic means, in nearly no time and very comfortably. In Germany this has therefore been made a criminal offence. In Section 22b StVG (German Road Traffic Act) [32], a law has been put into place that forbids the production of programmes that allow for such manipulation as well as passing them on. The threat of punishment is up to one year of jail, and the software and hardware can be confiscated. Of course the readjustment of mileage might be necessary if the mileage counter has been replaced. If the intention lies in repairing and not manipulating the mileage, it is permissible to obtain and use the necessary equipment (hardware and software). The same will apply to any manipulation of speed-limiting devices that are compulsory in heavy commercial vehicles.

2.2.3 Unauthorised Points of Interest in Digital Maps

The possibility to display Points of Interest in digital maps has been available for quite some time, and it is definitely a function with additional value that is not to be criticised in itself. However, if the Points of Interest programmed in the map allow for warnings before passing by stationary radar control units (or common grounds for radar controls), the benefit of such control units in terms of road safety is considerably diminished.

As an example of the legal situation concerning such warnings, the Germany case shall be described. It must, however, be pointed out that such a law is not necessarily in place in other Member States of the EU. In many countries no regulations against such warnings exist.

In Germany, a device that allows for such warnings in vehicles is considered to be a device banned according to Section 23 paragraph 1b StVO (German Road Traffic Code) [33]. This not only applies to devices that have some kind of sensor to detect a radar or laser control unit, but it even covers navigational systems with location information on stationary radar control units. Even though these devices are banned, they can be sold freely – even in Germany – as there is no law against owning such a device either. It is only their use that is banned.

Of course such devices could be banned altogether. This, however, would call for an EU-wide regulation as the right to move goods freely throughout the EU will not allow for a single national prohibition. The free movement of goods is one of the most important rights of EU Policies. This was established through the Customs Union/Cooperation as well as the Prohibition of Quantitative Restrictions between Member States. Most important in this context is Article 34 of the Treaty on the Functioning of the European Union [36], which guarantees the import and sale of any product that has rightfully been produced within a Member State of the EU by prohibiting any restrictions on imports or measures of equivalent effect between Member States. However, in case such a device containing information on (stationary) radar control units is carried in a vehicle in Germany and this is discovered, e.g. in a stop-and-search operation of the police, it can be confiscated and destroyed as its use is banned (see above). In the case of navigational systems (even only a nomadic device and not a device fixed to the car itself), it is, however, doubtable whether confiscation would still be a proportional measure, as the device only offers the warning as an additional feature and the main function is navigation. Hence considerable difficulties exist when applying this law to the new threats of an implementation of radar unit location data as Points of Interest in navigation systems.

It should further be mentioned that according to the German Federal Court of Justice, on the basis of private law, the purchase contract of such a radar warning device is considered to be against public policy which results in the contract becoming void. However, this has hardly any effect in practice as the device remains in possession of the buyer, and only the contractual rights, such as warranty or guarantee, cannot be enforced by law. Nevertheless claims for warranty or guarantee, might well be accepted by the manufacturer even if these rights cannot be enforced.

2.2.4 Unauthorised TV, DVD or Internet Access in Moving Vehicles

Devices for playing DVDs are available at very low prices and can easily be fitted in standardised mounting slots in all kinds of vehicles. They usually tend to have monitors that arm out so that the video can be viewed on a large scale monitor.

Since Terrestrial Digital Video Broadcasting (DVB-T) is available, it has become possible to watch TV even at high speed in vehicles. According to test reports available over the internet, reception quality is ensured at speeds up to 160 Km per hour.

In the near future, access to the internet will generally be available as an option in cars as well. After-market solutions might be available too.

All these functions are uncritical as long as they are meant for passengers, e.g. children on the rear seats. Even the front-seat passenger can focus his/her attention on such devices at no risk at all, even when the car is in motion. If, however, such entertainment or information facilities are accessible to the driver when going any faster than walking speed, dangers for traffic safety are immanent as the attention of the driver – and especially his visual attention – must not be distracted from surrounding traffic.

In practice, such options fitted as original equipment will switch off as soon as the car goes any faster than walking speed, as car manufacturers are well aware that the driver's attention might otherwise be distracted with negative consequences for safety. However, possibilities to manipulate such an automatic "switch-off" for the driver do exist. Over the internet, detailed information on how to short-circuit the "switch-off" has been available in the past. For more recent cars, for which the possibilities for manipulation have already been considerably minimised by OEM's, electronic boxes are already available that facilitate manipulation. The dangers that such devices might further create, e.g. by interfering with other safety-relevant vehicle electronics, is another source of danger in this field. As far as nomadic devices with entertainment functionalities are concerned, an automatic switch-off is usually not foreseen in the first place.

From a legal point of view, consequences are only very implicit. This is mainly due to the fact that such possibilities for entertainment have previously not been available at all, and legal provisions in this respect are therefore not in place. For example, in Germany the driver is therefore only generally required to ensure full view on the surrounding traffic according to Section 23 paragraph 1, sentence 1 StVO (German Road Traffic Regulations) [33]. This must not be impaired. It is, however, only a theoretical possibility to prosecute distractions, as it would be very challenging to prove that a driver

was actually distracted. The existence of the possibly distracting screen itself is not banned in Germany. The only available possibility on the national level lies in the prohibition of use in vehicles, and this again would prove impossible to enforce. Therefore, once again, the most favourable way to achieve traffic safety in this respect is to make sure that the manipulation of an automatic “switch-off” is barred. As a first step, the automatic “switch-off” must, of course, be implemented, but this is presently not available in all nomadic devices.

2.2.5 Other Possibilities for Intentional Manipulation

As described in section 2.1.5, it must be supposed that many other possibilities for manipulation exist. Most examples tend to be too specific for the concerns of this report. One rather representative example is the manipulation of the convertible top. This will allow for opening the top of a convertible when driving at considerable speed. Here it must legally be questioned whether the danger for safety is so fundamental that this leads to an annulment of the vehicle’s operating licence. This manipulation, however, has strong technical implications and cannot be assessed legally as long as the real-life dangers are unknown.

As soon as awareness of manufacturers to such new dangers is raised, the risk is usually assessed and counter-measures are put into place. So far resulting risks are in many cases unknown, and this applies to the manipulation of the convertible top. Cases of substantial dangers resulting from other possibilities for manipulation are presently not known.

A possible future risk of high impact might be the manipulation of Driver Assistance Systems. The manipulation of systems that actively intervene into driving comprises the greatest dangers. The legal consequences of such manipulations are difficult to assess and would be very complex.

Presently, however, such risks of Driver Assistance System manipulation can only be supposed and no information is currently available. Here manufacturers have a vital interest in avoiding any negative impacts on traffic safety. Measures to bar manipulation are therefore already in place. Their effectiveness can be assumed as long as such dangers remain absent.

2.3 Typical Measures Taken by OEMs

The use of electronic systems in vehicles has been increasing for years to fulfil safety, environmental and comfort requirements for current and future vehicles. Being informed is an important issue for today’s customers. However, manipulation and misuse could be dangerous when it comes to changing the original features of the “regulated” and safe car. For this reason, vehicle manufacturers have developed feasible security mechanisms to meet current and future demands.

An overly detailed discussion of potential technical measures may well create situations which provide information to potential hackers who intend to change the data or software of in-vehicle or special infrastructure systems and thus actually support their intentions. Furthermore, any detailed presentation of actual technology could stimulate new ideas for illegal actions, manipulation or misuse. Therefore the measures described below are presented in a very broad manner to emphasise how very much aware the automotive industry is of potential security risks and eventualities.

The industry has consistently striven to always stay one or more steps ahead of potential hackers. These strong efforts from the OEMs serve to enhance the effectiveness of such systems and complicate the potential fraud against electronic systems of different vehicles.

The automotive industry sees the need to differentiate between the various systems which produce safety, environmentally and legally relevant information and comfort functions. Not all functions can be treated in the same way.

With regards to security, the industry needs to make distinctions between the different functions, applications and communication channels, such as:

- More than one internal bus system physically separated by gateways acting as firewalls
- Various ways to enter the vehicle's internal systems
- General and personalised applications
- Usage over more than a decade
- Communication with common and individual partners
- Fast and slow communication.

The industry thus focuses on developing solutions which are most suited to the function under consideration of several given boundary conditions and needs. This also means that it may well

occasionally be ineffective or impossible to fulfil all requirements through one feasible solution. Therefore, not all security requirements can be fulfilled equally with the respective technology.

To create an effective set of security measures, the industry uses principles which are listed in the following examples:

- Division of electronic applications into different domains
- Use of gateways and firewalls
- Authentication of external equipment for access to the vehicle
- Use of digital signatures for protection against unauthorised manipulation.

In particular, with regards to communication applications for all principles, the necessary infrastructure needs to be implemented, which in some cases needs to be operated world-wide and must therefore be developed extremely carefully and in the most “secure” manner.

For this reason, there can be no general standard to assure the necessary security function. Furthermore, the final responsibility for management of the vehicle security has to lie with the OEM concerned. This also hampers any chances for manipulation between vehicle models and brands. In fact, a certain minimum level of security may be required whereas the technical realisation shall lie within the responsibility of the OEMs.

2.3.1 General Characteristics: Unauthorised Enhancement of Engine Power

With regards to power enhancement, we need to consider a number of situations, such as:

- Power enhancement is extremely difficult if not impossible to detect from outside the vehicle.
- The power output of an engine is type approval relevant.
- When changing the power output of an engine, other specifications and values will change at the same time. These have a direct impact on the durability of the powertrain and various components.
- Power enhancement within a limited range is possible by changing components or engine application maps. If no development activities to clarify durability issues took place, there would be extremely high risks of costly engine or powertrain break downs.
- Authorised power enhancement is technically possible, if all the necessary requirements are fulfilled.
- Clearly, it is very much in the interest of the OEMs to avoid unauthorised power enhancement.

The OEMs develop and implement solutions which can restrict, impede or considerably hamper the engagement in the engine control unit, and its integration and change of the related datasets for the engine maps, whilst taking into account the legal, product liability and/or product characteristic issues.

In addition, other measures may be considered:

- protection against manipulation of software and datasets
- avoiding any exchange of engine controllers and associated control units through internal safeguarding and authentication of system components and software if, for example, a controller exchange or software update is necessary
- individualisation of software, controller and data through special software keys
- the utmost care in granting access authorisation for service issues concerning software, data or relevant components.

The automotive industry takes great care to implement the necessary software components to avoid or hamper unauthorised engine power enhancement. Research and development activities as well as special working groups within the industry are currently seeking to establish specialised standards and provide feasible solutions.

2.3.2 Unauthorised Mileage Adjustment

The adjustment of the vehicle mileage has to be avoided in current and future vehicles. Strong efforts with electronic measures are carried out to prevent the mileage registration from being manipulated.

A number of different methods keep the real mileage through storing it in different locations and comparing the values. These methods use special algorithms which are also protected through patents and non-disclosure mechanisms. Fraud or manipulation can be discovered through special monitoring instruments which are normally available at the brand service centres.

At present, it seems nearly impossible to change the mileage values in new vehicles without detection. Reprogramming the data or changing the odometer will not produce such a desired result.

2.3.3 Unauthorised Points of Interest in Digital Maps

Additional services to support drivers and provide them with information in an easy manner are welcome and commonly used. This serves to reduce potential driver distraction and risk of accidents. One major service is to provide special Points of Interest, e.g. hotels, petrol stations, public locations and various other attractions. Further possibilities can provide individual information for the disposal of the user.

The provision of information is independent of the information content in all cases. There might be a selection of information which is defined by the means of data storage which is used in the vehicle. Most commonly this would be a CD or DVD which is used in the integrated navigation system, or other memory in various chip sets which can be filled with the required information chosen by the user. There is no way to distinguish between different types of information content.

At present, no technical measures exist to avoid the use of certain information or point of interest which are legally prohibited, or to differentiate between information items. An effective way to avoid the use of illegal information items and that type of misuse could be increased enforcement or awareness campaigns.

The legal situation in the different EU Member States and other key markets and countries needs to be evaluated and discussed carefully with regards to their legal effectiveness and infringement. However, this cannot be achieved via a technological solution.

2.3.4 Unauthorised TV, DVD or Internet Access in Moving Vehicles

The automotive industry complies with the legal requirement to prohibit activation of video and free internet access for all new vehicles moving beyond walking speed. In all new series production vehicles, the visual part of the video functions and the internet shall be switched off above a certain speed. This is relevant with regards to using the function from the driver's seat, whereas the services shall remain available for rear passengers.

For development purposes, special tools are required to enable additional functionalities which will not be available in new series production vehicles. These tools are only available for development engineers. Sensor signals containing data such as vehicle speed need to be distributed to different software packages and functionalities inside the vehicle architecture. Under the given conditions, it is necessary to be consistent and to use one type of sensor signal source to achieve high reliability. Furthermore, the high integration of the software and functionalities network in the vehicle may lead to communication errors if some sensor signals are manipulated. This may cause potential malfunction of functions, which in the case of manipulation the user would not accept.

However, under circumstances such as the available electronics architecture, encryption or encoding, bus structure, and cost, etc., it is impossible to avoid any illegal integration of external boxes or additional hardware to the wiring of a vehicle in order to change the various sensor signals. The result may be that other functions could also malfunction. Change of the electronics architecture in a vehicle through measures which may be able to avoid such manipulation may cause additional deficits or worse performance of other important safety functions.

This leads to the political question: What priorities are set according to the safety functionalities?

If the OEMs develop very strong countermeasures against vehicle manipulation of TV, DVD or internet functions, one simple and straightforward reaction of potential manipulators could be for the driver to use nomadic devices instead of the OEM equipment. This would eventually cause bigger safety problems than the current few manipulators. A solution which avoids the illegal use of nomadic devices therefore also needs to be considered.

2.3.5 Other Possibilities for Intentional Manipulation

Since various functions in a vehicle are supported by electronic means, some ideas might arise to manipulate these functions in order to enlarge the functional limits for comfort or performance of the system. Every electronic system or function in the vehicle could be a potential source for change within its application data.

The overall architecture and physical wiring system of a vehicle, which offers potential options for special modification, are so extremely complicated that any general supervision of the wiring is almost impossible with normal means. The important functions and systems, which can be defined through serious safety concerns or legal requirements, as well as those which may cause serious damage to the vehicle or injure the driver or passengers, are monitored to inform the driver if any malfunction occurs.

A lot of them could be switched off according to the choice of the driver or support the driver in the best possible way which is evaluated and developed by the manufacturer. Human-machine interaction, human behaviour or further boundary conditions are all considered in the design phase. Furthermore, the intended vehicle use and operation as learned and experienced by the driver provide further essential input to the design process.

If anyone intended to ignore such experience and act contrary to given rules, it would be impossible to prohibit via electronic means or to avoid manipulation through technical means in all cases. The range of different manipulation possibilities is so immense that general avoidance of such ideas would present a tremendous effort and would require huge resources for all cases. All functions which are considered necessary by the OEMs will be covered by monitoring. If others, e.g. the opening of the top of a convertible car, are functioning outside of the limits as intended by the manufacturer, the damage to other parts or the car body will prevent or reduce further safety risks without being dangerous to others.

Other functions, such as driver assistance systems which are today currently in research/development or in series production, are being discussed seriously within the OEMs. The responsibility of the OEM for the product leads to the development of solutions which are generally in line with the legal requirements and necessary product liability issues. Through this process, the necessary support functions for the OEM's intended use are generally implemented.

2.3.6 Manipulation of Speed Limiting Devices

Speed limiting devices are generally used in heavy commercial vehicles of the category N2, N3, M2, and M3. Passenger cars and related commercial vehicles of the category M1 and N1 do not use such devices. (See [31] for definition of vehicle categories.)

Any change of software or data for running the systems is protected in the relevant vehicles through various appropriate measures, such as:

- Using encrypted signals for speed information
- Monitoring relevant signals
- Using redundant speed signals and storing deviations as fault codes
- Following secure processes including authorisation keys for staff.

If there are provisions to increase the maximum allowed speed of a relevant vehicle, the user can change the gear rations of the transmission or the rolling circumference of the tires. In order to avoid such fraud, the revolution of the wheels under consideration of the dedicated tire models needs to be monitored. Another way to avoid speed of the vehicle to go above the allowed limits is to increase the enforcement of the illegal tire replacement.

2.3.7 Impact of Block Exemption

Within the field of automotive security, a lot of sensitive issues, data, and software components are handled and need to be protected in order to avoid unauthorised manipulation and fraud. To meet these goals, it is necessary to take care of the treatment of the relevant information for service and maintenance of such technologies in a secure way. The block exemption regulation stipulates that all relevant service and maintenance partners (branded and non-branded) have to be informed about necessary processes, data, software and keys to carry out the service, repair and maintenance work of the vehicle. For this reason it is essential for OEMs to develop solutions to ensure the required security and keep sensitive information within the realm of accredited stakeholders and partners. The automotive industry will continue to develop positions and proposals for feasible solutions.

2.4 Conclusion on Independent Vehicle-based Electronics

As described in the above sections, there are many measures taken by OEM's to increase the security of independent vehicle-based systems. Thus the negative impact, especially on vehicle's safety, promises to be reduced. It therefore seems justifiable to refrain from decisive measures in the field of independent vehicle-based electronics. That measures must remain proportional only support this finding. However, in case the eSecurity situation in the field of independent vehicle-based electronics should not improve, this issue must be reconsidered. In this case, it presently seems sensible to require a certain minimum level of security, with regulation only stipulating the end result.

As pointed out in section 2.2.3, not all threats can, however, be solved technically as certain applications necessarily need to be "open" in order to allow for their intended use. In order to tackle the issue of unauthorised Points of Interest in digital maps, an EU-wide regulation banning production and trading of such security threatening software, which is currently legal, may be a first step to be taken on the EU level.

3 Part 2: Interactive Systems

Two major problems have raised concerns in the ITS community:

- The privacy of vehicle location information which is used in location based applications. Such services raise privacy issues since they involve the collection, transmission and processing of information which could be related to individuals. Examples of such services are road charging and pay-as-you-drive insurance.
- The security and privacy of information in future cooperative systems applications which rely on vehicular communications and inter-vehicular communications. Examples of such applications include extended hazard warning in safety critical situations, applications to achieve high throughput in merging areas, extended blind spot applications, safe overtaking, and safe lane change assistance.

3.1 Security and Privacy in Location-based Applications

This section provides an analysis of security and privacy of location information in location-based applications based on two services: road charging and pay-as-you-drive. A great deal of attention has been paid to these two services recently. Since they are excellent cases for demonstrating the advantages of privacy by design, they are the main focus of this section.

3.1.1 Road Charging Service

3.1.1.1 Introduction

Road pricing or electronic fee collection is an application to charge a fee for using an infrastructure like roads, tunnels or bridges. This toll is meant to finance the maintenance of the infrastructure, for traffic management purposes, or for the reduction of negative environmental effects. The toll can depend on time, distance and place, and certain vehicle specific parameters, like the total weight, the number of axles, the existence of a trailer, and the emission class.

In Europe, tolls are collected from Heavy Goods Vehicles (HGV > 3.5 tons) or private cars by electronic or manual systems. Manual systems are comprised of car tax stickers which allow access to a network for a certain period of time, or the purchase of tickets for a specific route on the network.

Electronic systems are comprised of systems which may or may not require the installation of On-Board Equipment (OBE). Systems without OBE can make use of automatic number plate recognition. For electronic systems which use OBE, EU directive 2004/52 [39] allows three different technologies: 5.8 GHz microwave communication (Dedicated Short Range Communication - DSRC), satellite positioning, and GSM/GPRS mobile communication. With the advantage of being a free-flow system, the use of satellite positioning is recommended for future systems. These systems do not require the installation of road-side infrastructure for tolling purposes and can therefore be considered very flexible for any future demands, and in particular useful for large and lower-level networks.

In Europe, different toll schemes have been implemented:

- Area pricing: the toll is charged for the time stayed or the distance driven in a zone (e.g. time-based London congestion charging, and distance-based tolling system for HGVs in Switzerland)
- Section pricing: the toll is charged for driving on a certain section or several connected sections of a network (e.g. the HGV toll on motorways in Germany and Austria)
- Cordon pricing: the toll is charged for crossing a cordon on specified points (e.g. city tolling in Stockholm).

Currently three countries make use of satellite positioning for their tolling systems: Germany and Slovakia as primary source for toll detection, and Switzerland for validation of the odometer results. Most countries in Europe still use DSRC-based systems, e.g. France, Spain and Italy. Countries like the Czech Republic already have a DSRC-based system in place for tolling on motorways but are planning to introduce a satellite-based system for tolling the lower-level network of federal and municipal roads.

It is expected that the Member States will introduce more electronic tolling systems, in particular for heavy goods vehicles, to raise money for maintenance of the traffic infrastructure, to steer traffic, and to reduce negative impacts of traffic like congestion or emission. Within the limits of applicable EU legislation, the decisions on the introduction of tolling systems, on the technology, and on the tolling parameters remain at the individual Member States.

To foster a seamless transport system for Europe and to support the transport industry, EU directive 2004/52 introduced the European Electronic Toll Service (EETS) which allows a user to pay his tolls in all electronic toll systems in Europe using only one OBE and having only one contract with a so-called EETS-Provider.

3.1.1.2 Implementation and Privacy Issues

Electronic systems collect data necessary to determine the toll due to invoice the user, to enforce the toll regulation, and finally to check the operation and performance of the system.

EU Directive 2004/52 sets the following requirements for the EETS for processing of data: “Member States shall ensure that processing of personal data necessary for the operation of the European electronic toll service is carried out in accordance with the Community rules protecting the freedoms and fundamental rights of individuals, including their privacy, and that, in particular, the provisions of Directives 95/46/EC [37] and 2002/58/EC [38] are complied with.”

Privacy issues need to be considered for all kind of toll systems, but they are of particular relevance for satellite-based systems. The used positioning data is sensitive information as it could potentially allow a third party to trace a person’s movement and speed.

The basic steps of processing of tolling relevant data in satellite-based systems are:

- Determination of the location, based on received satellite signal (probably combined with information from other sensors like odometer or gyrometer)
- Detection of the toll object (like a road segment or an area) by comparing the measured positions with the geometry of the toll objects (geo-referencing)
- Calculation of the toll based on the detected toll object, time, vehicle and contract parameters
- Aggregation of several toll declarations and invoicing the user.

Several different implementation strategies have been developed to support this process. The following main designs have been tested and implemented in road-charging systems, each having its own advantages and disadvantages.

1. **Thin Client**

   The OBE mainly collects positioning information from a satellite signal (and other sensors) and transfers it to the back-office system for further processing. In some implementations, not every individual position will be transferred, since algorithms on the OBE compress the information and select the relevant information for the toll object detection, which can lead to a substantial reduction of data. This supports efficient use of the communication channels.

   This scenario can lead to reduced complexity on the OBE side but requires enough bandwidth on the communication channels and a high level of availability of the back-office systems.

   The OBE itself cannot decide whether it is on a tolled network or not. Therefore all positions need to be transferred to the back-office system where they are matched with the actual toll objects.

   From a privacy perspective, this is not an appealing scenario as the server receiving all of the data would indeed have a complete picture of every meter driven by the vehicle (even on non-toll roads), and could even derive further data, such as speed. More consideration is needed to determine whether such a scenario complies with general privacy requirements like data minimisation and data avoidance. Many national laws only allow collecting data if absolutely needed for a specific purpose.

   Technical solutions exist to send positioning data using pseudonyms to the back-office system and to reveal the identity of the OBE only when the geo-referencing process detected that the OBE is on a toll road network. However, still large amounts of data are collected and discarded afterwards. It is questionable whether trust of the users can be established in such a system.

2. **Thick Client**

   In the case of a thick client, the process mentioned above is performed inside the OBE. It is even possible to claim the payment (e.g. by allowing credit card payment with the OBE).

   The only information which has to leave the OBE is any invoice relevant data. This can be as little as a monthly fee for the use of the toll road network by a particular user.

   This scenario should be favoured from a privacy perspective since only payment relevant data is leaving the OBE. However, it must be ensured that the toll operators still can check whether the user has met his obligations (e.g. the proper declaration of variable parameters like number of axles) and that the processing results of the OBE are correct. Implementation of data security measures and certification procedures can create the trust in the system.

This scenario requires more intelligence on the OBE and most probably more updates of tolling relevant data like geographical information of toll objects or tariffs. Compared to the thin client, this operational overhead is moderated by the operational advantages in case of the unavailability of communication channels or back-office systems. Thanks to their autonomy, thick clients are able to continue processing for a certain period time.

3. **Smart Client**

   The smart client scenarios can be placed somewhere between a full thin and a full thick client scenario.. The smart client takes advantage of being able to distribute intelligence between OBE and the back-office systems according to the needs of the actual system.

   As an example, a smart client could perform the detection of toll objects on the OBE and send the recognised toll objects to the back-office system where tariff operations are done. This reduces complexity on the OBE, takes operational advantage of the flexibility of a back-office process and preserves the privacy of the user. However, in this scenario the toll objects still need to be transferred to the back-office.

   No implementation strategy has been prescribed for operators and future providers of national schemes or the EETS. The decision for a strategy therefore is with the operator of the national tolling system or the EETS Provider, as long as the decision complies with the general requirements on user's privacy.

   A proper balance needs to be found between the demands of the user and the toll operator. On one hand, the user has a legitimate demand in having his privacy respected. On the other hand, the toll operator has an interest in getting paid for the use of the toll road network and in checking the compliance of the users and toll service providers with the toll regulations.

   From a privacy perspective, the preferred solutions should, if possible, avoid collecting unnecessary data and respect the principles of data avoidance and data minimisation.

3.1.1.3 Conclusion on Road Charging

Electronic toll systems create a continuously increasing contribution to the funds for financing Europe's road infrastructure and to traffic management. With the advance of electronic tolling solutions throughout Europe, in particular of satellite-based tolling systems, addressing privacy issues is of utmost importance to ensure trust in the system.

A privacy-by-design approach has to be applied when designing road charging systems. A concertation must be set up between road charging implementers, road charging policy makers, and privacy policy makers to ensure a common approach for ensuring the users privacy.

For all electronic systems, the following basic principles should be accepted as a general policy and need to be implemented through all processes and components of the tolling system:

- Data shall be collected, transmitted and processed only as far it is necessary for creating claims or enforcement purposes.
- Data shall be collected, transmitted and processed only for the purposes created by corresponding laws or by a private contract in accordance with applicable EU and national privacy laws.
- Data shall be processed and transmitted using proper data security measures.
- Data shall be deleted or made anonymous when no longer needed for claiming or enforcement purposes.

Adherence to these rules respects not only the privacy of the individual user of the tolling system. It also raises the general acceptance of tolling systems as a means for financing our transport infrastructure.

3.1.2 Pay-as-you-drive Service

3.1.2.1 Presentation

Insurance represents a large portion of the cost of owning a car. In order to lower costs for both owners and insurers, insurance companies have developed Pay-As-You-Drive (PAYD), or Pay-Per-Mile models. In contrast to the current pay-by-the-year policy, customers are charged depending on where and when they drive, instead of a fixed premium per year. For each kilometre that a car is driven, the statistical risk of accident is calculated and translated into a personalised insurance fee. A PAYD contract clearly lays out the exact fares for driving under different conditions depending on the type of road, time of day, etc. For instance, driving during rush hours could be more expensive than driving at other times, or driving on a highway could be more expensive than using secondary roads.

Pay-As-You-Drive insurance models are hailed as the future of car insurance due to their advantages for users and companies [17] [18]. First, the insurance fees applied to each user are fairer than the ones in the pay-by-the-year scheme, as customers are only charged for the actual kilometres they travel. Customers can also reduce their monthly bill by choosing cheap itineraries and/or times, or by just not using their car. This makes vehicle insurance affordable for lower-income car users (e.g. young people) or for people who wish to have a second vehicle. Second, PAYD policies are socially beneficial. They improve road mobility and encourage responsible driving which decreases the risk of accidents, which in turn saves money for users and insurers in addition to saving lives. Finally, PAYD has an environmental benefit, as it reduces traffic jams and discourages driving, hence reducing energy consumption and pollution emissions. For these reasons many companies have started PAYD programs (see [19] [20] for a summary and a comprehensive list of these companies, respectively).

3.1.2.2 Implementation Issues

Although PAYD insurance seems to have many advantages, its current implementations involve an inherent threat to a user's privacy. In most of the implemented schemes, the full information used for billing, such as the time and position where the car was, is gathered by an electronic unit ("black box") in the car. It is then transferred to the insurance company and, in some of the cases, to a third company providing the location and/or time data to the transportation infrastructure. This situation has a downside both for the companies and the customers. For the company, managing these huge databases creates the risk of information leakage [21] [22] and the consequent damage for the company in terms of cost and/or reputation with the public. For the client, the main disadvantage is that the possession of location and time data allows the insurance company to track almost every movement of a car over time with ease and precision. Iqbal and Lim [23] show how GPS data can be automatically analysed to produce profiles of a driver's behaviour, social activities and work activities, thus conflicting with the proportionality principle as the data collected provides far more information than is necessary for the provision of the service. For instance, in their study they could identify the home location of a subject in the experiment in four out of five cases. For the fifth case, the error in the prediction stemmed only from the fact that the car was parked in an underground parking lot instead of in front or near the actual home.

Some companies claim to provide privacy preserving PAYD schemes, as they collect only statistics about the location data, e.g., how much time a driver was driving on a highway, but not when or on which highway. However, these statistics are sometimes handled by a third party who collects and keeps the raw location data, hence the threat to privacy does not disappear but is only shifted. As a result, insurance companies and/or third parties can build vast databases of location data. For instance, Octo Telematics [24] claims to work for more than 30 companies in Europe and to have had more than 866,000 clients in October 2009. Even if the third party has no knowledge of the identity of the drivers, their home and work addresses can be easily identified from the trajectories and linked back to them [25] [26].

The data is transmitted through third parties, such as a telecommunications provider or a third party location data provider. Once the location data has been transmitted to a third party, the data subject has little control over it. This data could be stored or retained for long periods as well as used for purposes other than the ones for which it has been collected. Although Data Protection legislation may impose limits on what can be done with it, the penalties for breaching them are often very light. An option would be to further process the data after an anonymisation process. However, as mentioned before, anonymisation of location data such that it cannot be linked back to a person with high probability is very difficult, and researchers have not yet found a solution for this problem.

For the current PAYD implementations, the responsibilities for the processed data are not clearly defined. It is necessary to define whether the data subject is the car or its driver, or in some cases the owner (who can differ from driver in case of rental or company cars). The data processor is also not a clear figure as third parties and telecommunications providers as well as the insured car itself have access to, and sometimes process, the location data. Finally, a certification process and a specification of the functionalities of the black box need to be developed to ensure that neither companies nor users are liable for client misbehaviour or bugs in the box firmware.

3.1.2.3 A Privacy-Friendly Implementation

A possible solution for the provision on privacy in Pay-as-you-drive services follows closely the current implementation architecture, with the exception that the raw and detailed GPS data are never provided to third parties, as in the PriPAYD scheme presented in [19]. The main advantage of PriPAYD is that the insurance company receives only the billing data instead of the exact vehicle locations and thus cannot invade the user's privacy, while being sure it is receiving the correct data. The client can check that only the allowed data is entered in the insurance company database, and the raw data is available

for the client to check the correctness of the bill in case of a dispute between user and insurer. It is important to delineate the threat model.

There is little point for a Pay-as-you-drive system to try to protect user's privacy beyond what road users already expect today, thus one can assume that any third party adversary that has extensive physical control of the car will be able to track it by simply installing their own tracking system. The objective of PriPAYD is to limit casual and/or deliberate surveillance by the insurance company or any third parties with limited physical access to the car, as well as preventing the aggregation of a mass of location information in centralised databases. Fine grained location/timing information should be hard to obtain for any third party except the policy holder, who has the right to audit the bill and ensure its fairness. This protection still allows for surveillance of the drivers (in case they differ from the policy holders), but we are satisfied that no systemic surveillance risk is introduced beyond what is already possible today.

The PriPAYD design in [19] safeguards the *privacy of the policy holder* and the *integrity of the billing information*. Yet some attacks against the availability of the PriPAYD (or previous PAYD schemes) cannot be prevented while using cheap, off-the-shelf technology such as GPS and GSM. The design attempts to detect that such attacks are taking place, but how they are dealt with is dependent on the agreement between the insurance company and the policy holder, and appropriate actions or penalties must be codified in the contract to deal with them.

The key difference between PriPAYD and the current implementation of PAYD is that all computations transforming the GPS data into billing data are performed in the vehicle's black box. The data involved in the calculation of the final premium are the number of kilometres travelled, the hour of the day, the road the user has chosen, and the rate per kilometre given by the insurer (following the Octo Telematics model [24]). To perform the conversion, maps have to be available to the black box, and calculations have to be performed to match the coordinates with road types. These operations are no more complex than those already supported by any off-the-shelf commercial GPS navigation system. The rates imposed by the insurer or other policy parameters can be initialised in the black box when installing it, and they can be updated later in a trustworthy manner through signed updates.

Once the premium for a period of time is calculated, the amount to be paid, along with the current policy, is sent in a secure way to the insurance company via GPRS, or even cheaper SMS services. The data is signed and encrypted in a special way that allows the policy holder to check that only the minimum billing information is transmitted.

To ensure that the black box is not acting maliciously in favour of the insurance company, the car user or owner is allowed to audit the billing mechanism. For this purpose, we propose the use of an off-the-shelf USB memory stick. The data is recorded in an encrypted way on the stick so that only the policy holder can access it, and it is signed by the black box to ensure its authenticity and integrity such that it is usable as evidence.

A prototype of this scheme is presented in [27], where a proof-of-concept demonstrator is built in order to prove the validity and correctness of the design while showing that its functionality can be achieved within a reasonable cost. The results obtained after testing the prototype on a one hour trip around Leuven, Belgium suggest that privacy-friendly PAYD services are possible.

3.1.2.4 Conclusion on Pay-as-you-drive

Similarly to road charging applications, it must be taken into account that privacy has a major influence on the implementation of the pay-as-you-drive service. But a resulting privacy friendly implementation can involve the use of protection mechanisms which are novel in the ITS field whilst being well known by the security community. Consequently there is a need to gain deployment experience by testing these implementations in field operational tests.

3.1.3 Conclusion on Location-based Applications

- We have covered two location-based applications (road charging and pay-as-you-drive insurance) for which large scale deployment is currently planned, As a result, significant discussion has already taken place for each of them concerning privacy issues. From the results of these discussions, the following observations can be made:
- The complexity of security solutions requires agreement on evaluation criteria to evaluate solutions. Those criteria are needed to allow deciding stakeholders to make decisions (recommendation 4).
- Privacy cannot be an afterthought activity. Privacy by design is needed (recommendation 5).

3.2 Basic Legal Conditions for Interactive Systems

Exactly which elements characterise interactive systems (also referred to as “cooperative systems”) remains unclear at this point. This leads to the difficulty of being unable to state exhaustively which legal consequences interactive vehicle applications will create in the future. Furthermore, specific legislation does not currently exist in this new field. Therefore this section is limited to a more global view of the main legal issues affected:

- Section 3.2.1 highlights the most important legal aspects of privacy which will, as far as presently foreseeable, accompany the discussion on interactive systems and applications over the next years. The chapter describes why privacy will be an issue.
- Section 3.2.2 points out why other critical legal issues with a focus on liabilities are not currently expected to be relevant to interactive systems. Here a parallel is drawn to the discussion on Advanced Driver Assistance Systems (ADAS) over the past years.

3.2.1 The Privacy Issue of Interactive Systems

Some kind of Vehicle to Vehicle (V2V) or Vehicle to Infrastructure (V2I) interaction or communication is a main characteristic of future interactive systems. Along with this type of interaction or communication goes the handling of data beyond the boundaries of single vehicles. In such applications, data might thus be collected inside and outside of vehicles, transmitted to and processed in special units in order to, for example, provide the driver or other vehicle systems with additional information not otherwise available. The data processed for this purpose can feature information closely linked to the sphere of the individual driver as well as the passengers. Therefore data protection legislation or rights, generally referred to as privacy issues, must be met during the design process and when running such applications.

In section 3.1, the use cases on existing in-vehicle road traffic systems therefore illustrate the effect that the principle of ‘privacy by design’ may have on system architecture and circumscribe the legal measures that have been identified or taken in terms of privacy for specific applications in the past.

Future applications will increase the number of electronic systems processing data both inside and outside of vehicles. Therefore it is important to consider all personal data processing that a user will be confronted with, in both current and future systems, in order to assess specific demands for “privacy by design" in individual cases.

On the other hand, it is important to note that the processing of personal data as such is permissible according to existing data protection regulations. Much, however, depends on how this is realised in an individual case. As long as data protection is taken seriously in system design and operational structures, no insurmountable barriers in terms of privacy will be encountered when implementing applications. In this respect, electronic security (eSecurity) is an important instrument that can improve privacy considerably by securing the processing of personal data against illegitimate access.

3.2.2 Non-Privacy Legal Issues

Interactive systems serve a number of purposes such as traffic safety, improving mobility, environmental protection, and comfort. In most cases – and this is relevant in terms of applications in the focus of eSafety – the purpose is to influence “driving” in a very broad sense.

Such influence can be indirect via information provided to the driver. This is already the case with Driver Information Systems (e.g. navigation devices). Advanced Driver Assistance Systems (ADAS) goes one step further by assisting vehicle control. This assistance currently remains overridable at any time.

The legal situation for Driver Information Systems as well as ADAS has mostly been discussed in terms of the hampering effect the product liability risk will have. The PReVENT project [8] developed ‘Response3’, a Code of Practice on safe ADAS development that can substantially minimise factual risks in terms of product liability for ADAS. This is achieved by applying knowledge from the past to the design of new technologies. Simply stated, the idea is mainly based on maintaining ‘controllability’ so that the driver can take over control in case of malfunctions. It also proposes an organisationally safe development process which is described in detail. To a certain extent, this approach can be transferred to ‘interactive’ applications, even though the Response 3 Code of Practice was not initially issued for this purpose.

The development of interactive applications will, as is presently foreseeable, take the same development path and start off by simply informing the driver, and then at a later stage contribute to

the operation of “assisting” applications. This leads to the strong conclusion that interactive applications in vehicles will not bring about product liability risks too large to be handled.

However, what is new in the case of interactive systems is the existence of technical devices beyond the vehicle itself, e.g. computing at the roadside or within service-providing organisations that are possibly integrated into the wireless communication network. These technical structures will probably be at least as subject to failure as current purely vehicle-based systems. In case of failure, depending on the architecture chosen, the provider of these services might well run the risk of being charged with liability. This would, in most cases, be based on a negligent or intentional breach in the execution of a service provider’s duty. For example, in Germany such claims might be based on section 823 paragraph 1 BGB (German Civil Code) [35].

Yet this possibly critical finding must be considered with the above mentioned experience on Driver Information Systems and ADAS: Until now the driver must be considered responsible for driving. He is therefore obliged to react with attention to information, even if its faults are not immediately recognisable. Therefore any excessive reactions to information provided by ‘interactive’ applications that lead to damage must – as is the case for Driver Information Systems or ADAS – be considered contributory to the negligence of the driver. In most cases, this will, if not achieved otherwise, relieve the manufacturer as well as the service provider completely from being charged with liability.

Therefore the issue of liability is definitely existent but can be estimated to be manageable for the foreseeable Driver Information Applications and overrideable ADAS. A close assessment of the actual risk should, however, be made on the basis of every specific application’s design and designated architecture, as the rough estimation at hand can only be considered a first approximation.

It is therefore recommended to make further investigation on liability issues when interactive applications beyond informing systems, such as those with immediate impact on driving, are considered. This is needed to understand and monitor the effects that system-introduction will have.

3.3 Security and Privacy of Future Cooperative Systems

Currently, research projects like SAFESPOT [9] and CVIS [2] are preparing the next generation of ITS that will enable new kinds of applications that will make driving safer, more efficient, greener, and more comfortable. This will be enabled by the availability of a wide range of wireless communication technologies. Dedicated short range radio communication (DSRC), for example, enable vehicles to exchange messages with each other and with nearby Road-Side Units (RSUs). Alternatively, 3rd and 4th generation (3G and 4G) cellular networks may be used in some cases to implement the same kind of applications.

One example is a cooperative awareness application in which vehicles inform other nearby vehicles about their position and speed by means of broadcasted Cooperative Awareness Messages (CAM).

The COMeSafety [14] project has defined a reference architecture for such co-operative systems as depicted in Figure 1. Basically, a vehicle’s on-board unit (OBU) communicates with other OBUs, RSUs, personal mobile devices, and the central infrastructure using a wireless communication network. Note that all communication stations have a similar software architecture.

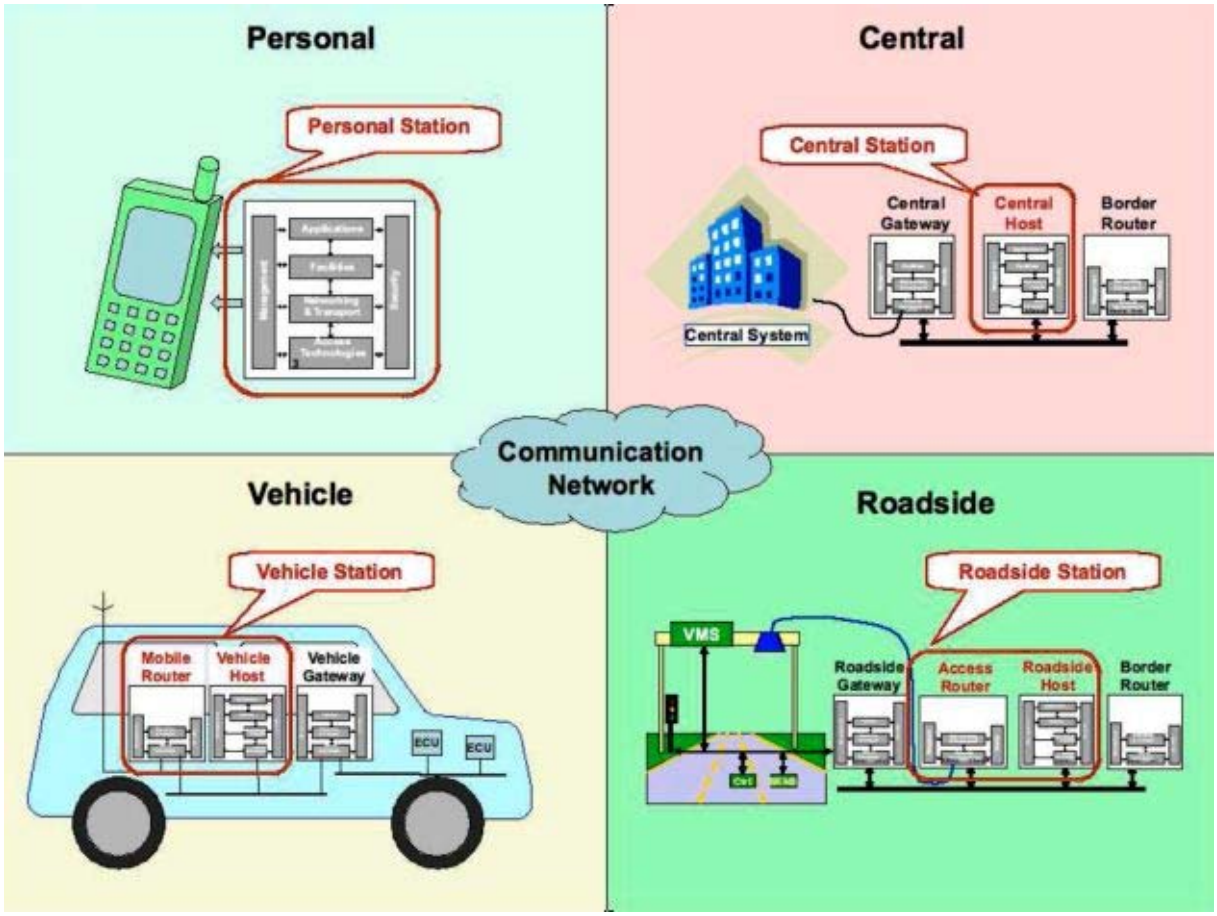

Figure 1: COMeSafety Reference Architecture

3.3.1 Analysis of Security Issues

Because we are dealing with a complex distributed system architecture, cases for security and privacy breaches are numerous. For instance,

- Since inter-vehicle hazard warning applications improve car safety, data transmission must be fast, robust, secure and reliable. It is essential to make sure that life-critical information cannot be modified by an attacker.
- Cooperative systems raise privacy issues for drivers and passengers. It is important to prevent easy location tracking of people, as well as the access to confidential data associated with people, e.g. medical records.
- Access to vehicles means easier access to the internal vehicle communication systems, which in turn raises intrusion issues. It is essential that the electronic components in the car are not modified, e.g. by changing vehicle parameters, or changing vehicle software. Software updates should be made securely.
- Nomadic devices could be connected to vehicles, and this could raise security issues. For example, can the nomadic device use the transmission channel made available for safety applications, or can the nomadic device contain safety related applications?
- Open communication platforms could have an impact on security and trust. Several research projects in the area are in progress, for example OVERSEE [5].
- The coexistence of multiple independent applications such as business and public applications raises trust issues in terms of sharing system assets, e.g. communication and execution resources, and of sharing application assets, e.g. information on a subscriber.

The use case approach applied earlier in this document cannot be followed because:

- Specific issues depend on specific solutions.
- A high level of technical detail will in general be involved.
- Security is typically scattered throughout a system over many components and many levels, which would result in a large number of use cases.

Therefore this section will use an analysis approach instead of the use case approach used in earlier sections.

A primary concern of computer security is to eliminate or mitigate risks. Risk can be expressed in terms of probability of an unfortunate event and its potential damage. Examples of damage are: losing money, distrust, and political damage. Unfortunate events happen mainly because of systems having vulnerabilities and people attacking those systems by exploiting their vulnerabilities.

Only real systems can have vulnerabilities. For this analysis existing cooperative systems were not considered; only their general communication architecture is discussed. Therefore this section will conclude with the enumeration of a list of threats that should be considered instead of vulnerabilities.

First a high level communication architecture will be discussed to set the context for cooperative systems. The next section describes the organisations and persons (actors) involved in cooperative systems. Finally this section will conclude with a list of typical threats for cooperative systems.

3.3.1.1 High-level Description of Co-operative Systems

A refined communication architecture of co-operative systems, inspired from existing initiatives (e.g. COMeSafety[14], CVIS [2], Safespot [9] and Coopers [1]) is shown in Figure 2.

A number of interfaces (lines) in this figure have been labelled. Circles indicate external access points for possible human interaction. The communication architecture consists of the in-vehicle and infrastructure subsystems represented by squares. In-vehicle subsystems are:

- **Vehicle Host**: This system is a platform for deploying applications in the vehicle. The platform will offer many common services (e.g. communication, security) and has a human machine interface (HMI).
- **ECUs**: Electronic Control Units (ECUs) are embedded units in the vehicle and are typically connected to the vehicle's internal bus. The car manufacturer is responsible for these units. These applications might provide information that is of interest to the applications on the Vehicle Host. Examples are vehicle speed or the state of the windshield wipers, which can be used as a (cooperative) rain detector. Typically there are many ECUs connected on several networks with different characteristics, e.g. entertainment and safety.
- **Applications on Vehicle Host**: These applications add services to the vehicle. In this report, typical safety applications are considered. However, projects like CVIS focus on cooperative applications to improve use and comfort also.
- **Nomadic devices**: Nomadic devices, e.g. Personal Digital Assistants (PDAs) or cell phones, might be an integral part of the system architecture. Applications on the nomadic device could benefit from the information, connectivity and infrastructure.
- **Other nearby vehicles**: This diagram box is not a new subsystem but represents another vehicle in the neighbourhood in reach of communication, which creates the Vehicle-to-Vehicle interface.

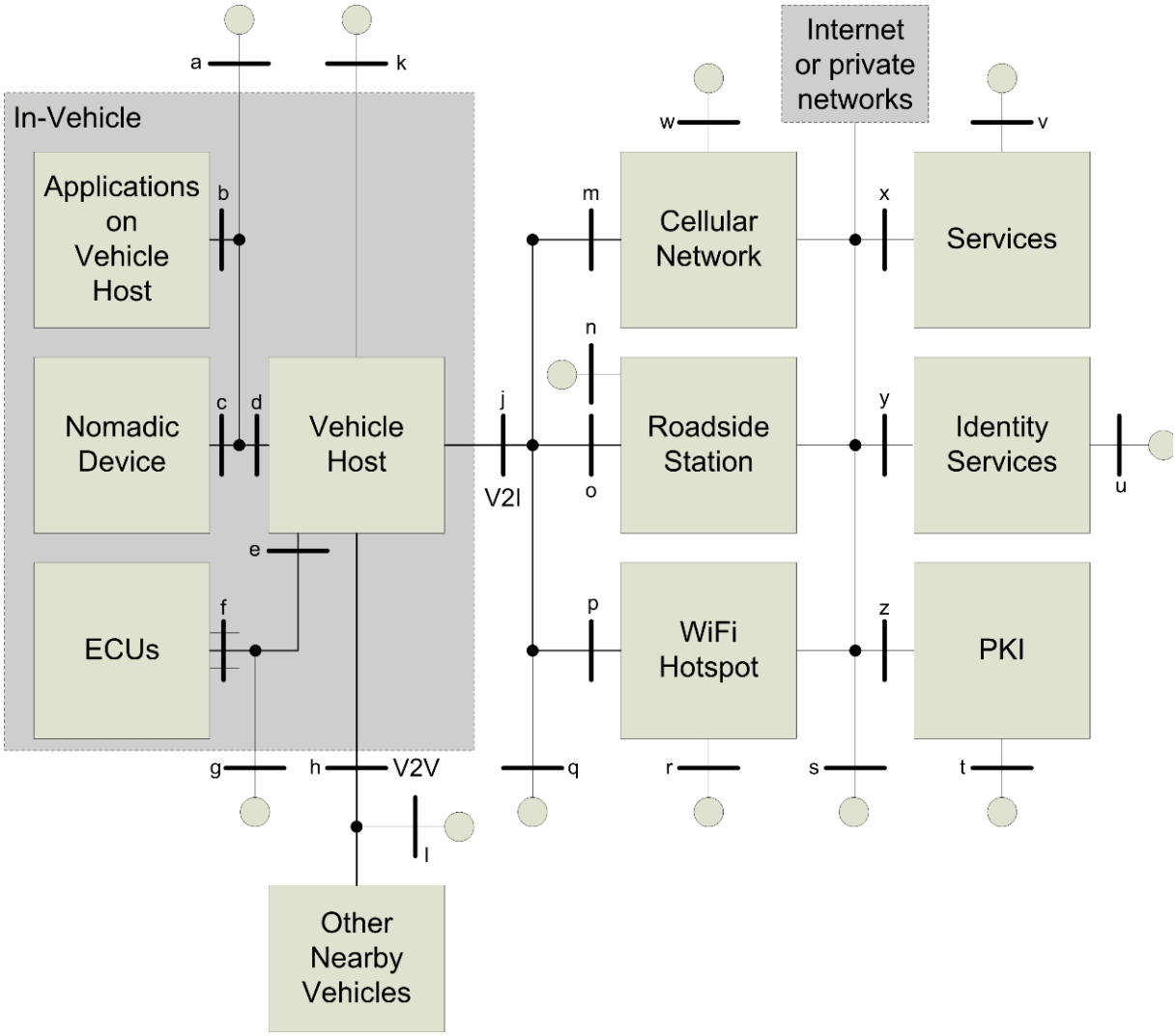

Figure 2: General architecture for vehicle IT infrastructure.

The infrastructure subsystems are:

- **Cellular networks**: This subsystem represents the infrastructure for mobile connectivity, such as GPRS, Universal Mobile Telecommunications System (UMTS).
- **Roadside units**: These subsystems are located beside the road and are able to communicate with local vehicles.
- **WiFi hot spot operators**: Like the mobile phone operators, this subsystem represents another party for realising connectivity between the vehicle and the infrastructure.
- **Identity service**: This subsystem represents the first entity on the infrastructure which a vehicle should connect to and log on to for checking credentials,. It also should hold all dynamic information of the infrastructure like subscriptions to services.
- **Service**: The service subsystem represents a set of commercial services, e.g. dynamic routing, or services from the government, e.g. road conditions. The vehicle driver or owner can subscribe to these services and automatically get the right application installed on the Vehicle Host.
- **PKI** (Public Key Infrastructure): When a PKI is used, a trusted party manages identity, keys and certificates and should interact with the infrastructure.

3.3.1.2 Actors

Actors are persons or organisations that have a particular role in scenarios concerning cooperative systems. From a security point of view, actors are considered potential attackers of systems. Typically actors have access to particular subsystems because of their role.

To find a list of actors and possible attackers related to vehicle communication systems, i.e. applications, platform and infrastructure, the life cycle of vehicles should be investigated. The following phases in the life cycle of a vehicle can be distinguished:

- Developing and manufacturing the vehicle
- Using and maintaining the vehicle
- Disposing of the vehicle.

Developing and manufacturing phase actors:

- **Original Equipment Manufacturer** (OEM): Initially vehicles have to be designed, assembled and tested by the OEM. The OEM is responsible for the quality and safety of the vehicle.
- **Suppliers**. Parts of the vehicles are designed and/or manufactured by suppliers of the OEM. Suppliers in the automotive industry normally cooperate closely with an OEM to produce high-quality products at low costs. Suppliers can be active in many fields. The stakeholders, however, focus on suppliers of hardware and software components that are accessible on the vehicles' internal buses.
- **Public authorities**: Public authorities are indirectly involved early in the lifecycle for various reasons such as legislation, type approval and public policy, e.g. safety, privacy, environment. Accredited testing organisations (see below) might be responsible for executing certain tasks.
- **Standardisation bodies**: Standardisation of security-related matters, e.g. risk management, security controls, protocols and algorithms, helps to improve the quality and interoperability of security aspects.
- **Accredited testing organisations:** Testing bodies are independent parties that should verify that products are produced and behave according to certain policies.

Usage and maintenance phase actors:

- **Dealer**: Vehicles will typically be sold through dealer networks. The vehicles are sold to the legal owners, i.e. companies or persons, which might be different from the vehicle user. Dealers will typically install equipment in the car to meet the requirements of the user and the government as part of the delivery. The vehicle communication systems might be initially commissioned (i.e. activated) by the dealer.
- **Vehicle owner:** The owner might subscribe to services. The services can be provided by commercial parties or the government.
- **Vehicle user**: The vehicle user, who could also be the owner, has access to the vehicle and its systems. He makes use of the services.
- **Mobile network operator**: In case the vehicle needs to communicate on the telematics infrastructure for services, a mobile network operator is involved for wireless data transmission.
- **Infrastructure operator**: A vehicle communication infrastructure is provided and maintained by the infrastructure operators.
- **Service provider**: Service providers use communications facilities to offer their services. They can be compared to an Internet Service Provider that gives us access to the internet.
- **Content providers**: Content providers are connected to the infrastructure and host useful applications. Depending on the nature of the organisation, the content can be either free, e.g. provided by government, or should be paid for, e.g. provided by a commercial organisation.
- **Road authorities**: Road authorities are responsible for road maintenance and operation. As commercial companies, road authorities may also provide services to vehicle users, like broadcasting local road conditions, travel time or route advice.
- **Technical inspection companies**: These organisations mainly focus on periodic inspection of the vehicles. Examples of relevant vehicle states are safety aspects and proper operation of mandatory equipment. In the future, some inspections may also cover the security behaviour of related systems or components, e.g. OBUs, using specific measures.
- **Service organisations**: These organisations are responsible for vehicle maintenance; therefore they have access to the car, to its equipment and to the internal buses of the vehicle.
- **PKI authorities**: These organisations are responsible for managing basic security-related services for the telematics infrastructure. Examples are keys, certificates, and their related identities.
- **Public authorities**: Some public authorities are also indirectly involved in this phase. They are, for example, responsible for legislation and other interests such as traffic management at a national level.

- **Criminals**: Criminals make money in many ways, for example vehicle theft, transportation of stolen vehicles, robbery of the driver, tracking and stealing valuable cargo. They might benefit from information from the vehicle communication system, or they might want to manipulate infrastructure of in-vehicle systems.
- **Malicious hackers**: Persons who have access to parts of the telematics infrastructure could try to interfere with legitimate entities. Access could be provided by various parts of the infrastructure, for example the internet, mobile communication networks, and wireless connections.

Disposing phase actors:

- **Vehicle owner**: Before disposing of the vehicle, the owner is involved in the decommissioning process.
- **Service providers**: During vehicle disposal, service providers might also be involved. For example, if an OBU is to be reused, the service provider should remove sensitive information on the OBU and decommission the system in the administration of the infrastructure.

3.3.1.3 Threats

It is important to realise that threats act on all architectural levels. Important levels are:

- Network level
- System level
- Application level
- Human level.

Because of the general nature of the communication architecture being discussed, it is only possible to come up with a list of general threats and vulnerabilities. The following list describes the majority of them:

- **Errors in the system**: Developers are the source of threats from errors. Most of the time the threat is unintentional. Threats from system errors might result in problems with data integrity or system stability which might create new system vulnerabilities.
- **Neglect**: When employees neglect their tasks or do not follow the mandatory procedures or security policies, it might create new system vulnerabilities or expose data.
- **System intrusion**: This class of threat is typically network based, but it can also occur on the local vehicle interfaces when system access is not protected properly.
- **Unauthorised system access**: Unauthorised people might get access to systems when systems are not properly protected, users use weak passwords, weak authentication devices are used, or passwords somehow become public, e.g. by social engineering. When unauthorised persons have access to a device, they can change its configuration, e.g. weaken firewall settings, add malicious applications or disable applications. This is true for both the in-car systems and infrastructure systems. Illegal access or a denial of service attacks on the internal vehicle buses could seriously compromise the safety of the vehicle.
- **Spoofing or impersonation**: Especially when communicating car-to-car, it is important to distinguish between legitimate and false entities. False entities might provide other vehicles with false information which might have an impact on safety. There are numerous other examples where authenticity of entities is very important.
- **Cloning or stealing an identity**: By cloning or stealing a valid identity, an illegitimate entity can be turned into a legitimate one, or at least one that cannot be distinguished from legitimate ones. When the gain is high enough, criminal organisations might invest a lot of effort to find ways of getting access to system keys, and thus the identity or other entities.
- **Denial of service attack**: This kind of attack is typically a network level attack. By saturating communication channels or by using a jammer, in the case of wireless communication, the result is that applications which depend on communication cannot function properly. It is be possible to do the same for the infrastructure part of the system.
- **Intrusion on personal privacy**: There are several methods to violate privacy regulations. Privacy sensitive data can simply be sniffed from the network when communication is not encrypted. A vehicle's location can be tracked by mobile telecom operators because they can track mobile communication devices in large areas. Another intrusion method involves services that use privacy sensitive data. This data should not be misused by the provider of that service.

- **Malicious code**: This threat is part of several of the previous threats, but it worth mentioning separately. Malicious code can be autonomous or it can be installed manually by an attacker. Malicious code might make a system unstable, provide backdoors for later intrusions, send data to systems of the attacker, or even participate in denial of service attacks. The malicious code can act at the system level or application level.
- **Time**: Time is a threat for several reasons. What is secure today can be regarded insecure in several years because of advances in technology for cracking secure algorithms. Key wear is also a factor. Whenever keys are used a lot for communication, eventually enough data can be assembled to reconstruct the secret keys.

3.3.2 Technical Protection Measures

3.3.2.1 Technical Requirements

Before looking at the solution space, we first need to identify the requirements for a technical solution that protects security and privacy in cooperative ITS. This section is based on work carried out within the EU ITS project SeVeCom [10]. Table 1 and Table 2 list the requirements and provide a short statement on their estimated importance with respect to eSafety applications.

Name	Short Definition	Estimated Importance
Integrity	Prevention of unauthorised data modification	Integrity of data plays a major role in eSafety applications, as maliciously modified data can cause a lot of damage.
Confidentiality	Prevention of unauthorised data disclosure	Confidentiality is not required for most eSafety applications, as related data is mostly public, e.g. warnings, that should be made public and not be kept confidential.
Availability	Prevention of unauthorised degradation or denial of system operation and data access	The importance of system availability depends heavily on the actual scope of applications and the reliance which people put on these systems. Whereas a careful driver can compensate for the failure of an optional warning application, the failure of an automated driving system would be disastrous.

Table 1: Key Security Requirements

Name	Short Definition	Esteemed Importance
Authentication	Corroboration of the claimed identity	For most eSafety applications, knowing the identity of communication partners is of secondary importance. Other aspects like attribute authentication are more relevant and discussed later in this section.
Access Control	Decision on granting access to services/data to authorised system entities	Most eSafety services and the data communicated between vehicles will be public, therefore authorisation/access control will be relevant only to a small number of closed (paid) applications. For in-vehicle systems, access control is a mandatory feature. Essentially, Access Control can be viewed as the aftermath of Authentication and Authorisation.
Auditability	The enabling of after-the-fact recording and analysis of system events	Depends on the kind of traceability that stakeholders mandate.
Non-repudiation	Proof of the originator of message/information to provide Accountability	Depends on the kind of liability properties that stakeholders mandate.
Privacy	Prevention of privacy infringement, i.e. disclosure of private data to unauthorised parties	Privacy is a major concern, especially in Europe, and a distinguishing feature compared to non-European activities.

Table 2: Additional Security Requirements

The provision of security in co-operative systems applications must in particular overcome a set of specific technical, economic, and social challenges:

- **Network scale and dynamics**: Vehicular networks will be the largest real-life instances of self-organised ad hoc networks. They also bring the challenge of mobility into the picture, as vehicles will not be able to participate in long-term security protocols because of the high dynamicity of the network. For example, two cars crossing each other on the highway have only few seconds to exchange information which is mainly safety-related.
- **Privacy**: One of the major consumer concerns about the Vehicle Communication (VC) technology is its potential influence on privacy.
- **Trust**: A key element in a security system is trust. This is particularly emphasised in vehicular networks because of the high liability required from safety applications and consequently from the vehicles running these applications. Co-operative systems will involve many stakeholders, and the presence of the human factor will increase the probability that misbehaviour arise.
- **Cost**: Cost is another inhibitive factor in the deployment of VC solutions. In fact, the introduction of new communication standards for vehicular communications will require manufacturers to install new hardware modules on all vehicles, thus increasing the unit cost for consumers. Another costly addition will be the infrastructure that will allow VC functions, e.g. to access on-line authorities as part of a security service such as authentication. These costs should be minimised while keeping sufficient support for vehicular networks applications.
- **Gradual deployment**: The time span of VC deployment until it reaches considerable penetration is around a decade. This means that only a small proportion of vehicles will contain the enhanced features of VC over the next couple of years. Yet, this functionality should still be supported despite the low penetration rate. This also applies to security services where, for example, protocols should be performed without the widespread existence of roadside infrastructure.

Based on this understanding of requirements, the approaches for security and privacy protection for cooperative ITS will now be discussed.

3.3.2.2 Approaches

Different research projects have addressed the issue of security and privacy protection in co-operative systems to come up with solutions. The FP6 project SeVeCom extensively analysed security and privacy issues in V2V and V2I systems and proposed a baseline architecture that provides basic security and privacy mechanisms. Other projects like IEEE 1609.2 [30] and Network On Wheels (NOW) [4] also proposed security mechanisms for V2V or V2I systems. The basic building blocks of all those approaches are very similar. They will be described based on the SeVeCom baseline architecture.

Furthermore, the FP7 project PRECIOSA [6] is addressing privacy in cooperative ITS, and the FP7 project EVITA [3] is defining a secure in-vehicle platform providing a secure base for cooperative systems.

Altogether, these projects provide a substantial set of results and proposals that could be used in cooperative ITS. Their results directly go into standardisation and Field Operational Test (FOT) activities like the security working group of the Car-2-Car Communication Consortium (C2C-CC)[13], working group 5 (focusing on security) of the ETSI technical committee on ITS [29], and the security architectures of SIM-TD [11] and PREDRIVE-C2X [7] FOT projects.

Figure 3 gives an overview of the SeVeCom baseline architecture and prototype implementation. It shows the major components needed for securing cooperative ITS. The *Security Manager* controls and configures a number of security components that are responsible for the following security functions:

- **Identification & Trust Management Module**: This manages the long-term identity certificate of a vehicle and is also responsible for the verification of remote certificates.
- **Privacy Management Module**: This is responsible for managing the pseudonyms of vehicles. Pseudonyms are a concept where the identifiers used for authentication of vehicles do not include any data that allows linking the identifier to a specific vehicle or driver. These short-term IDs are to be used instead of long-term IDs and are to be changed regularly to prevent the creation of complete itinerary tracks of vehicles. The responsibilities of this module include changing pseudonyms (and correlated identifiers in the communication stack) and providing new pseudonyms when old ones expire or are not to be used any more.
- **The Secure Communication Module**: This contains components that are specific to certain communication patterns or protocols and are dedicated to protecting confidentiality, integrity, or availability of a specific form of communication, i.e. by applying digital signatures, encryption, or consistency checks as needed.

- **In-Vehicle Security Module**: This controls the connection between the on-board unit and other in-vehicle networks and ECUs by means of firewalls, intrusion detection systems, or similar mechanisms. Its purpose is to prevent successful attacks on other in-vehicle systems in case of OBU compromise.
- **Crypto Support Module**: All crypto operations and the protection of secret key material are encapsulated in the Crypto Support Module.
- **Hardware Security Module**: The Crypto Support Module includes a Hardware Security Module that provides extra protection to secret key material so that it cannot be accessed even if an OBU is compromised.
- **Hooking Approach**: In order to connect the security subsystem to the rest of the communication stack, SeVeCom applies a so-called hooking approach. Inter-Layer-Proxies (ILPs) introduced between the different layers of the communication stack allow the components of the secure communication module to register and get notified in case of certain events, e.g. a packet passing between layers. They can then take appropriate actions, e.g. attach/verify signatures or check the consistency of packet content.

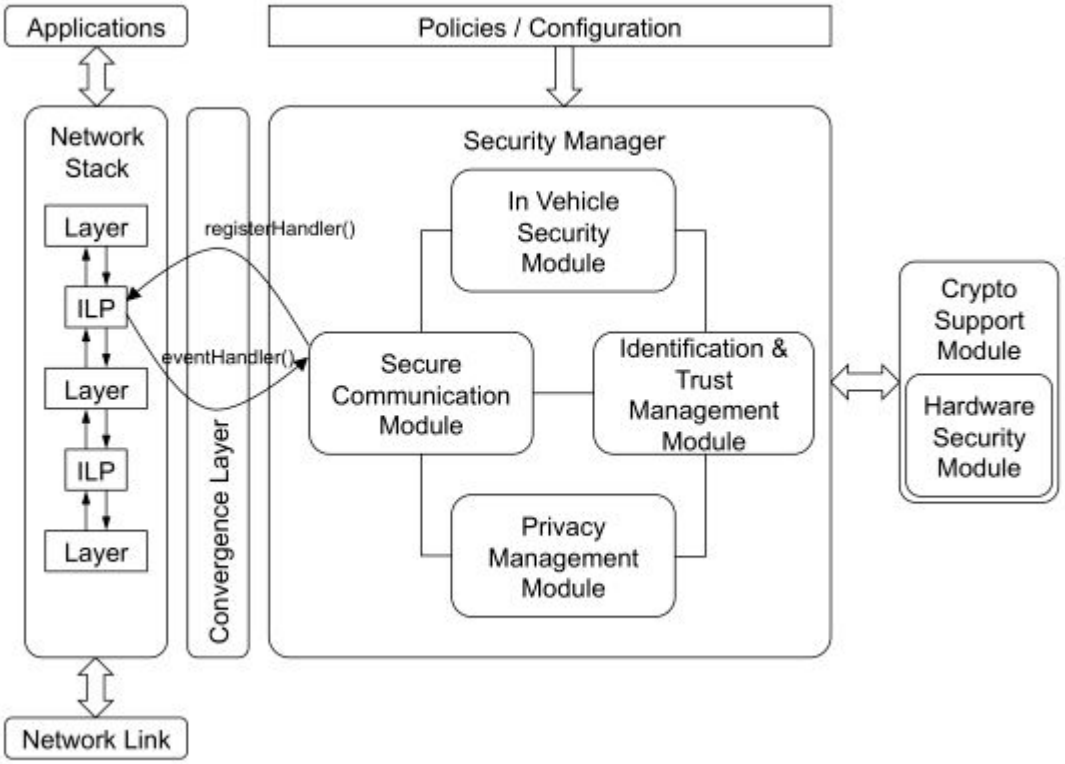

Figure 3: SeVeCom Baseline Architecture

Other projects refine this architecture and focus on certain aspects. For example, the PRECIOSA project [6] proposes refined pseudonym management and additional mechanisms to enforce privacy policies in cooperative ITS systems, focusing also on backend systems where data is collected, aggregated, and processed. The later policy enforcement system leverages on trusted computing components and a policy control monitor to ensure that only policy-compliant access to personal data is possible.

The EVITA project [3] provides a strong in-vehicle security architecture and trusted computing components. Those components can be deployed as a Hardware Security Module as specified in the SeVeCom Baseline Architecture.

From the SeVeCom Baseline Architecture, one can identify the most relevant and commonly proposed technical components needed for the security and privacy of cooperative ITS:

- **ID Management and Authentication Mechanisms:** This ensures the authenticity of vehicles. In most approaches, this includes asymmetric cryptography based on elliptic curves, certificates issued by a trusted third party or certification authority, and digital signatures to authenticate messages.

- **Privacy Protection:** By means of a *Pseudonym System*. Here, a balance has to be found between authentication and privacy requirements. This includes the question of whether a "lawful intercept"[2] mechanism is required to resolve pseudonyms to long-term identifiers, thus removing the anonymity provided by the pseudonyms under certain well-defined conditions. A second approach to enhance privacy protection can be the application of a *Mandatory Policy Enforcement* scheme where privacy policies can control what data processing is allowed on data.
- **Secure Communication Mechanisms:** These are usually specific to certain forms of communication. Currently, standardisation and FOT efforts focus on simple Cooperative Awareness Messages (CAM) and Distributed Emergency Notification Messages (DENM) that are sent as link-layer broadcasts. Here, message signing is usually the most relevant security mechanism. Still, it needs to be noted that other communication patterns like Geocast, Position-based Routing, Advanced Information Dissemination, or Aggregation also require more advanced protection mechanisms.
- **Data Consistency Checks:** These try to verify the correctness of disseminated information, e.g. by applying certain plausibility checks to position or speed information.
- **Efficient Cryptographic Operations** and **Protection of Secret Key Material**: These are partly implemented by means of a Hardware Security Module.
- **Protection of the In-Vehicle System**: These are implemented by security gateways between the OBU and other in-vehicle systems, but also by providing security mechanisms in the vehicle to ensure overall system integrity.
- **System and Architecture Integration**: This is a special challenge as the security mechanisms need to be closely integrated with the communication system and sometimes also with the application.

3.3.3 Organisational Measures

Organisational measures could also be put in place for various reasons, such as the following:

- As an intrinsic protection mechanism. For instance a company operating an information system could set up a hierarchical clearance procedure to ensure that only accredited persons access and modify some critical application data.
- As an accompanying measure to the use of an underlying technology. For instance the use of public/private keys necessitates the operation of a public key infrastructure.
- As a means to verify that a given level has been reached. For instance, the design of a privacy-by-design application could follow a design process that could be evaluated. Likewise, interoperability, security protection, privacy protection features of a subsystem could be verified through various approaches, such as internal quality insurance, and certification.

It is not possible at this stage to identify and finalise organisational measures, because there are too many unknowns in the way co-operative systems will be deployed. However it has become clear that concertation measures need to be put in place in due time to discuss and agree on such measures, possibly during field operational test phases.

3.3.4 Conclusion on Future Cooperative ITS Applications

As we have seen, future cooperative ITS will pose many challenges on the organisational, legal, and technical levels. This is due to the fact that those cooperative and dynamic systems include many participants from a legal, organisational, and technical point of view, and there are no or only a few central entities controlling such systems.

While research projects and different groups like the eSecurity Working Group [15], the Article 29 Working Party [12], or the security group of the Car-2-Car Communication Consortium have started addressing those issues, there is still significant work to be done before cooperative ITS is ready for deployment.

On the legal side, applicability of current laws has to be analysed in detail. In particular, a discussion is needed on whether current data protection laws that target mostly data processing in businesses can be applied to such decentralised forms of data processing.

From an organisational point of view, responsibilities for security and data protection in cooperative ITS have to be clarified. There are different potential candidates, like suppliers, OEMs, vehicle owners, and drivers. It needs to be determined whether there is even a need to clearly assign such responsibilities by appropriate laws or regulations. Furthermore, technical protection measures will

[2] During the final review of the report, some readers have pointed out that there is actually no legal basis for such measures.

require appropriate supporting mechanisms, e.g. a Public Key Infrastructure (PKI). The responsibilities for the structure of such mechanisms need to be clarified. For example, it is currently unclear who would operate and finance such a PKI system. The organisational challenges of running a PKI for potentially millions of vehicles in Europe and even beyond must not be underestimated.

From a technical point of view, there is already a rough consensus on how to secure at least initial and simple forms of cooperative ITS. The next required steps are to harmonise, classify, and select existing mechanisms. This cannot be done by only the ITS security community. Instead, all stakeholders must participate to answer important questions on the set of applications to be deployed, the desired protection levels, acceptable costs, and political and legal constraints. Groups like the Car-2-Car Communication Consortium, the ETSI Technical Committee on ITS [29], and the eSafety Forum [14] provide the appropriate framework for such discussion and other important decisions.

To avoid delaying the market introduction of cooperative ITS just because of missing security and privacy protection solutions, there is a pressing requirement to evaluate and demonstrate their effectiveness in scenarios that exceed the level of the earlier research projects. Field Operational Tests (FOTs), including strong security and privacy parts, should analyse the performance, scalability, effectiveness, and practicability of those proposed mechanisms. In addition, a clear vision of integration into the overall cooperative ITS architecture is required, based on a close cooperation between architecture and security groups (recommendation 6.2).

It must also be noted that not all aspects of the proposed mechanisms are fully understood. Examples include performance effects of security mechanisms, e.g. message signatures, on the overall communication system, and the actual level of privacy achieved by pseudonym solutions. To avoid unpleasant and costly surprises after market introduction, upcoming FOT projects should also address remaining research issues that do not analyse how to achieve a certain security or privacy goal, but instead focus on the consequences that introducing such security mechanisms will have on the overall system. Such research has been neglected up to now.

Finally, there needs to be awareness that current standardisation and testing activities focus for good reasons only on a very limited set of communication mechanisms and applications that basically include one-hop link layer broadcast and a small set of basic applications. Protecting such systems and applications is a challenge in itself. However, there should also be a long-term research vision that ensures that research on security and privacy protection mechanisms for next generation cooperative ITS is conducted in time to ensure a smooth transition to even more advanced driver assistance systems or even automated driving. Two examples of such systems are securing advanced forms of communication or cooperative driving applications, and ensuring the privacy of drivers in applications that are highly personalised and include personal profiles.

In summary, it is recommended to maintain further work related to cooperative systems (recommendation 6). In particular:

- Ensure standardisation and harmonisation of security solutions.
- Quickly converge on a basic set of security and privacy protection mechanisms based on a careful selection of existing proposals. Then evaluate the scalability and effectiveness of such mechanisms in real-world systems and gain a deeper understanding of the effects that such mechanisms will have on the overall system. Address consequences of the security mechanisms on the overall hardware. FOT projects can provide the right framework for this analysis if and only if security and privacy are addressed as central project elements and are not just “add-ons”.
- Be aware that current work is only focusing on a small subset of the whole potential of cooperative ITS. Therefore, especially for security and privacy research, a long-term research focus that goes beyond the current relevancy for first generation systems needs to be ensured.

4 Recommendations

The following recommendations are made by the eSecurity working group:

1. Ensure separation between independent vehicle-based systems and interactive systems. Vehicle based systems should remain under the responsibility of the OEMs and should not be affected by interactive systems
2. Investigate liability issues of applications beyond informing systems (systems that have an immediate impact on driving). Further research work is needed to understand and monitor these effects
3. Harmonise legal measures in place within Member States concerning improvement of electronic security (e.g. regulations on manipulation of mileage). Today inconsistencies among legal framework within the Member States exist.
4. Address security issues raised by specific applications. In particular define evaluation criteria and methods which stakeholders can use in their decision process.
5. Undertake further work to identify further recommendations for a privacy by design approach.
6. Maintain further work related to cooperative systems. In particular,
   - 6.1 Ensure necessary standardisation and harmonisation of security solutions.
   - 6.2 Validate security and privacy mechanisms for the first generation of cooperative systems in field operational trials.
   - 6.3 Undertake research activities on security and privacy issues for the next generation of cooperative systems.

The table below shows the scope of each recommendation.

		Technical scope	**Legal scope**	**Organisational scope**
1	Ensure separation between independent vehicle-based systems and interactive systems	XX	X	XX
2	Investigate liability issues of applications beyond informing systems	X	XX	
3	Harmonise legal measures concerning improvement of security		XX	
4	Address security issues raised by specific applications and define suitable support measures		X	XX
5	Discuss further recommendations for privacy by design	XX	XX	XX
6	On-going work needed for cooperative systems	XX	X	XX

X indicates a normal presence in a scope category.

XX indicates a strong presence in a scope category.

5 Glossary

Term	Definition
3G, 4G	3rd Generation, 4th Generation of cellular wireless standards
ACC	Adaptive Cruise Control
ADAS	Advanced Driver Assistance Systems
CAM	Cooperative Awareness Messages
CAN-Bus	Controller Area Network Bus
C2C	Car-To-Car communication
C2I	Car-To-Infrastructure communication
C2X	Car-To-Any communication
C2C-CC	Car-To-Car Communication Consortium
CAM	Cooperative Awareness Messages
CC	Common Criteria
CD	Compact Disc
DENM	Distributed Emergency Notification Messages
DSRC	Dedicated Short-Range Communications
DTC	Diagnostic Trouble Code
DVD	Digital Versatile Disc
DVB-T	Terrestrial Digital Video Broadcasting
EC	European Commission
ECE, or UNECE	Economic Commission for Europe, or United Nations Economic Commission for Europe
ECU	Electronic Control Unit
eCall	Emergency Call
ECDSA	Elliptic Curve Digital Signature Algorithm
EDPS	European Data Protection Supervisor
EETS	European Electronic Toll Service
ERI	Electronic Registration Identification
eSafety	Electronic Safety
eSecurity	Electronic Security
ETSI	European Telecommunications Standards Institute
EU	European Union
FIPS	Federal Information Processing Standard
FOT	Field Operational Tests
FP6	Sixth Framework Programme of the EC
FP7	Seventh Framework Programme of the EC
GNSS	Global Navigation Satellite System
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile communications
HGV	Heavy Goods Vehicle
HIS	Hersteller Initiative Software
HMI	Human Machine Interface
ICT	Information and Communications Technology
IVC	Inter-Vehicle Communications
IEC	International Electrotechnical Commission
ILP	Inter-Layer-Proxies
ISMS	maintaining Information Security Management Systems
ISO	International Organization for Standardization
ITS	Intelligent Transport Systems
ITSEC	Information Technology Security Evaluation Criteria
IVC	Inter-Vehicular Communication
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology

OEM	Original Equipment Manufacturer
MSD	Minimum Set of Data
OEM	Original Equipment Manufacturer
OBU	On Board Unit
PAYD	Pay As You Drive
PKI	Public Key Infrastructure
PDA	Personal Digital Assistant
POI	Points of Interest
PSAP	Public Safety Answering Point
RSU	Road Side Unit
RTD	Research and Technology Development
SMS	Short Message Service
StVG	Straßenverkehrsgesetz: German Road Traffic Act
StVO	Straßenverkehrsordnung: German Road Traffic Regulations (or Highway Code)
StVZO	Straßenverkehrs-Zulassungs-Ordnung: German Road Traffic Licensing Regulations (or Road Traffic Act)
TC	Technical Committee
TV	Television
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
V2C	Vehicle-To-Car communication
V2I	Vehicle-To-Infrastructure communication
V2V	Vehicle-To-Vehicle communication
V2X	Vehicle-To-Any communication
VC	Vehicular Communication
VIN	Vehicle Identification Number

6 References

Projects and Working Groups

[1] Project Coopers http://www.coopers-ip.eu/

[2] Project CVIS http://www.cvisproject.org/

[3] Project Evita http://www.evita-project.org/

[4] Project Network On Wheels (NOW) http://www.network-on-wheels.de/

[5] Project OVERSEE https://www.oversee-project.com

[6] Project Preciosa http://www.preciosa-project.org/

[7] Project PREDRIVE-C2X http://www.pre-drive-c2x.eu

[8] Project PReVENT http://www.prevent-ip.org/

[9] Project Safespot http://www.safespot-eu.org/

[10] Project SeVeCom http://www.sevecom.org/

[11] Project SIM-TD http://www.simtd.de

[12] Article 29 Data Protection Working Party http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

[13] Car-2-Car Communication Consortium (C2C-CC) http://www.car-to-car.org/

[14] COMeSafety Coordination Initiative http://www.comesafety.org/

[15] eSecurity Working Group http://ec.europa.eu/information_society/activities/esafety/forum/esecurity/index_en.htm

[16] eSafety Forum http://ec.europa.eu/information_society/activities/esafety/forum/index_en.htm

Publications

[17] T. Litman, “Distance-based vehicle insurance feasibility, costs and benefits,” Victoria Transport Policy Institute, Tech. Rep., 2007. http://www.vtpi.org/dbvi com.pdf

[18] F. Zahid and C. Barton, “Pay per mile insurance,” Davenport University, Tech. Rep., 2004

[19] C. Troncoso, G. Danezis, E. Kosta, and B. Preneel, “PriPAYD: Privacy Friendly Pay-as-you-drive Insurance”, Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society

[20] S. Minguijon-Perez, “Pay as you drive directory. http://payasyoudrive.wordpress.com/

[21] Alert as 170000 blood donor files are stolen, February 2008. http://www.independent.ie/national-news/alert-as-170000-blood-donor-files-are-stolen-1294079.html

[22] Norwich Union Life fined £1.26m for security holes, December 2007. http://www.theregister.co.uk/2007/12/17/ norwich_union_life_fsa_fine/

[23] M. U. Iqbal and S. Lim, “An automated real-world privacy assessment of GPS tracking and profiling.” in Second Workshop on Social Implications of National Security: From Dataveillance to Uberveillance, 2007, pp. 225–240

[24] Octo Telematics S.p.A. http://www.octotelematics.com/solutions/insurance-telematics/

[25] P. Golle and K. Partridge, “On the Anonymity of Home/Work Location Pairs”, in Pervasive 2009

[26] J. Krumm, “Inference attacks on location tracks,” in Pervasive, 2007, pp. 127–143

[27] J. Balasch and I. Verbauwhede, “An Embedded Platform for Privacy-Friendly Road Charging Applications.” Under Submission to Design, Automation and Test in Europe (DATE 2010), 2009.

Standards, Directives, Laws, and Treaties

[28] Standardisation Initiative Car-2-Car Communication Consortium http://www.car-to-car.org/

[29] Standardisation initiative. ETSI Technical Committee on Intelligent Transport Systems (TC ITS). http://www.etsi.eu/WebSite/Technologies/IntelligentTransportSystems.aspx

[30] IEEE 1609.2 Standard http://www.standards.its.dot.gov/fact_sheet.asp?f=80

[31] Vehicle Categories:
http://www.acea.be/images/uploads/rf/DEFINITION_OF_VEHICLE_CATEGORIES.pdf

[32] Section 22b of StVG (German Road Traffic Act): http://www.verkehrsportal.de/stvg/stvg_22b.php

Full StVG law: http://www.gesetze-im-internet.de/stvg/index.html

[33] Section 23 paragraph 1b of StVO (German Road Traffic Code):
http://www.verkehrsportal.de/stvo/stvo_23.php

Full StVO law: http://www.gesetze-im-internet.de/stvo/index.html

[34] Section 19 paragraph 2 of StVZO (German Road Traffic Licensing Regulations):
http://www.verkehrsportal.de/stvzo/stvzo_19.php

Full StVZO law: http://www.gesetze-im-internet.de/stvzo/index.html

[35] Section 823 paragraph 1 of BGB (German Civil Code) http://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html#BGBengl_000P823

[36] Consolidated version of the Treaty on the Functioning of the European Union (Treaty of Lisbon), Part 3 Union Policies and Internal Actions, Title II Free Movement of Goods, Chapter 3 Prohibition of Quantitative Restriction Between Member States, Article 34: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0001:01:EN:HTML

[37] Article 30 of Directive 95/46/EC The Data Protection Directive:
http://www.dataprotection.ie/viewdoc.asp?DocID=94

[38] Article 15 of Directive 2002/58/EC Concerning the processing of personal data and the protection of privacy in the electronic communications sector:

http://www.aedh.eu/Directive-2002-58-EC.html

[39] EU Directive 2004/52 on the interoperability of electronic road toll systems:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:166:0124:0143:EN:PDF